Digital Citizenship Policy Development Guide

Digital Citizenship Policy Development Guide

This document is available on the Internet at:
http://education.alberta.ca/admin/technology/research.aspx. Copyright © 2012 Crown in Right of the Province of Alberta, as represented by the Minister of Education.

Permission is hereby given by the copyright holder to use, reproduce, store or transmit this material for educational purposes and on a non-profit basis. However, Crown copyright is to be acknowledged. If this material is to be used, reproduced, stored or transmitted for commercial purposes, arrange first for consent by contacting:

School Technology Branch
Alberta Education
10th floor, 44 Capital Boulevard
10044-108 Street, Edmonton, AB T5J 5E6
Telephone: 780-427-1091 (toll free in Alberta by dialing 310-0000 first)
Fax: 780-415-1091

ALBERTA EDUCATION CATALOGUING IN PUBLICATION DATA

Alberta. Alberta Education. School Technology Branch.
Digital citizenship policy development guide.

Also available online: http://education.alberta.ca/admin/technology.aspx

ISBN 978-1-4601-0350-0 (Print)
ISBN 978-1-4601-0351-7 (Online)

1. Information society – Government policy – Alberta.
2. Education – Effect of technological innovations on.
3. Technological literacy – Alberta – Citizen participation.
4. Internet in education – Alberta. I. Title.

HM851.A333 2012 303.4833

Legal Advisement

The intention of this guide is to provide a support resource. It is not intended to provide legal advice. As always, readers should ensure they have sought professional legal advisement on all policy related matters.

Acknowledgements

Name	Role	Organization
Dr. Lucy Miller	Chief Superintendent	Calgary Catholic School District
Mr. Gary Strother	Superintendent Area D Schools/Information Technology	Calgary Catholic School District
Ms. Karen Ryhorchuk	Communications Specialist	Calgary Catholic School District
On behalf of participating CASS members: Ms. Kath Rhyason	Executive Director	College of Alberta School Superintendents
Ms. Tanni Parker	Assistant Superintendent Student Learning Services	Edmonton Public Schools
Mr. Roger Clark	Superintendent of Schools	Fort Vermilion School Division #52
Ms. Kathryn Kirby	Assistant Superintendent of Teaching and Learning	Fort Vermilion School Division #52
Ms. Sharon Barrett	Learning Tools Support Coach	Fort Vermilion School Division #52
Mr. Bevan Daverne	Superintendent of Schools	Golden Hills School Division #75
Dr. Maurice Hollingsworth	Researcher/Author	Learning Designs Inc.
Mr. Barry Litun	Superintendent of Schools	Lethbridge School District #51
Ms. Wendy Fox	Associate Superintendent	Lethbridge School District #51
Mr. John Percevault	Director of Technology	Lethbridge School District #51
Mr. John Loree	Director of Curriculum	Lethbridge School District #51
Ms. Ellie Elliott	Superintendent of Schools	Livingstone Range School Division #68
Mr. Stephen Harris	Assistant to the Superintendent	Livingstone Range School Division #68
Dr. Bette Gray	Executive Director (Acting)	Learning and Technology Resources Sector, Alberta Education
Ms. Karen Andrews	Director (Acting)	School Technology Branch, Alberta Education
Ms. Edna Dach	Education Manager	School Technology Branch, Alberta Education
Dr. Larry Jacobs	Chief Superintendent of Schools	Wolf Creek Public Schools
Mr. Gary Spence	Assistant Superintendent	Wolf Creek Public Schools

Members of the Wolf Creek Public Schools U21C Committee		
Mr. Jay Cottell	Technology Integration Consultant	Wolf Creek Public Schools
Mr. Greg Esteves	Humanities Teacher	Wolf Creek Public Schools
Ms. Karen Klassen	Assistant Principal	Wolf Creek Public Schools
Mr. Nolan Krauss	Principal	Wolf Creek Public Schools
Mr. Mark McWhinnie	Technology Integration Director	Wolf Creek Public Schools
Mr. Don Wielinga	Principal	Wolf Creek Public Schools

Table of Contents

Executive Summary 1

Preface 2

Definition of Terms 2

School Authority 2

Policy 2

Social Networking Sites or Social Networking 2

Web 2.0 or Educational Web 2.0 2

Cloud Computing 2

What is the Purpose and Value of this Guide? 3

What are the Societal Level Considerations? 3

1. Introduction to Digital Citizenship 4

Provincial Initiatives: Digital Citizenship Policy Context 4

Inspiring Education: A Dialogue with Albertans 4

Policy Insights 6

Defining Digital Citizenship 7

The Need for Digital Citizenship Policy 9

Compliance or Commitment 11

2. Method 13

Research Methods 13

3. Understanding Digital Citizenship 14

Acceptable Use Policies Relative to Digital Citizenship Policies 14

Acceptable Use Policies 15

Digital Citizenship Policies 15

Digital Citizenship Policy: A Foundation for Digital Citizenship Instruction 16

Policy Insights 16

4. A Digital Citizenship Policy Framework 17

Digital Citizenship Policy: Nine Elements 18

1. Digital Access 18
2. Digital Commerce 19
3. Digital Communications 20
4. Digital Literacy 25
5. Digital Etiquette 26
6. Digital Law 27
7. Digital Security 32
8. Digital Health and Wellness 35
9. Digital Rights and Responsibilities 36
The Nine Elements: A Thematic Approach 37

Current Digital Citizenship Policy Issues 38
Cloud Computing 38
Bring Your Own Devices and Digital Citizenship Policy 43

5. Digital Citizenship Process and A Road Map 46
Leadership 46
Stakeholder Involvement 46
Digital Citizenship Policy: Three Layers 47
Policy Outcomes 52
Road Map to Digital Citizenship Policy Development 53

6. Conclusion 55

7. Resources 56
Background Resources 56
Policy Resources 56
Digital Citizenship Resources 58
Online Safety and Empowerment Resources 59
Security Resources 59
Instructional Resources 60

Appendices 61

Appendix A: Context 62

Policy Context: A Broad Societal Perspective 62
Policy Insights 64

Utilization Trends 64
Policy Insights 67

Provincial Context 68
Alberta SuperNet 68
Emerge One-to-One Laptop Learning Initiative 68

Bullying and Digital Citizenship 70
Policy Insights 71
Appendix B: ISTE NETS for Digital Citizenship 72
NETS for Students 72
NETS for Teachers 72
NETS for Administrators 73
Appendix C: Personal Information: A FOIP Definition 74
Appendix D: Digital Citizenship Needs Assessment 75
References 76

Executive Summary

Education leaders are re-examining acceptable use policies in light of the increasing use of highly mobile information technologies. While acceptable use policies were developed to manage and control behaviour, a digital citizenship policy takes a more comprehensive approach by recognizing the important role of education in preparing digital citizens. The intent of this guide is not to ascribe policy, but rather to offer guidance to leaders as they strive to better meet student and organizational needs. The guide provides an overview of digital citizenship policies and practices. It draws from research and the practical experience of Alberta schools.

The Digital Citizenship Needs Assessment Tool provides an overall sense of school authority readiness and provides specific guidance across a comprehensive set of 11 different areas. These 11 areas are rooted in research from Ribble (2011), and include:

1. Digital Access: Full electronic participation.
2. Digital Commerce: Online buying and selling of goods.
3. Digital Communications: Electronic exchange of information.
4. Digital Literacy: Process of teaching and learning about technology and the use of technology.
5. Digital Etiquette: Standards of conduct or procedures online.
6. Digital Law: Responsibility for actions and deeds using electronics.
7. Digital Security: Electronic precautions to protect learners, staff and organizations.
8. Digital Health and Wellness: Physical and psychological well-being in a digital world.
9. Digital Rights and Responsibilities: Freedoms extended to those in a digital world.

Two additional areas include:

10. Cloud computing: Transparently accessing networked servers across the Internet.
11. Personally owned devices: Student-owned or staff-owned technologies including smartphones, laptops and notebooks.

Each of the 11 areas includes a description, a series of considerations and questions to assist policy developers. These elements are included within the Digital Citizenship Policy Needs Assessment to help policy leaders determine their preparedness and status with regard to such policy.

Digital citizenship is a complex subject matter. It is the intent of the current guide to bring shape to this domain through questions and considerations that may be weighed by leaders. Through this process, the current work will assist leadership and stakeholder decision-making, guiding the development of effective digital citizenship policies.

Preface

Definition of Terms

It is important that a few terms be defined for use in the context of this guide. This will ensure better communication with the reader and clarify use of terms that sometimes vary.

School Authority

The term *school authority* or *authorities* references school authorities operating under a board of trustees. In some instances this equates to the term *school district* or *school jurisdiction*, but also accommodates those school bodies not encompassed by geographic bounds.

Policy

Within this work, the term *policy* encompasses all elements of regulation within the school authority. This includes over-arching board-approved policy, administrative regulations and associated guidelines. While some school authorities clearly articulate policy as strictly meaning board-approved regulations, other authorities use the term in a more general sense. There is not a universal definition of the term, so within this work, the term will encompass all regulatory documentation – from board policy to administrative regulation and supporting guidelines.

Social Networking Sites or Social Networking

The terms *social networking sites* or *social networking* in this context references sites that are used predominantly for social or connection purposes. This includes such sites as Facebook, Google+, Twitter and LinkedIn. Social networking is enabled through a website that lets users communicate among social groups through text, photos, video and audio.

Web 2.0 or Educational Web 2.0

Web 2.0 or *Educational Web 2.0* references sites that use the Internet for sharing content, communications and collaboration with a focus on educational value for learners and other participants. These sites include such learning tools as Wikispaces, Blogger, Edublogs, YouTube, VoiceThread, Wordpress and a significant host of other applications.

Cloud Computing

Cloud computing refers to the use of remote servers across the Internet (not school authority servers) to store, manage and process data. Cloud computing can be public wherein the service is available to anyone or it can be private wherein the service is sold to a limited number of people.

Note: While the distinction between the terms *social networking* and *Web 2.0* are often equated, for the purposes of this work, it is helpful to distinguish the differing intents and associated connotations.

What is the Purpose and Value of this Guide?

1. To assist school authorities in developing a digital citizenship plan and policies to address the needs of students.
2. To provide guidance in policy development to help protect students working in open, collaborative, online environments.

What are the Societal Level Considerations?

When considering digital citizenship policy development several layers come into consideration. This includes broad societal level considerations, such as:

- How students utilize highly connected mobile devices in an ongoing manner in their personal lives;
- Technologies bring learning value to educational contexts and align well with contemporary pedagogical approaches, thus creating highly adaptable students capable of working in a global context;
- Education systems face increasing pressures to incorporate contemporary technologies, including Web 2.0 technologies, enabling communications beyond the classroom, beyond the school and often beyond the country;
- Friedman's *Flat World* (Friedman, 2005), where employers seek learners with skills in collaboration, communication, critical thinking and creativity (Kay & Greenhill, 2013); and
- The knowledge that today's workplace assumes relatively deep knowledge of contemporary learning approaches as the demand for skills shift from routine to non-routine tasks.

1. Introduction to Digital Citizenship

Provincial Initiatives: Digital Citizenship Policy Context

Several provincial initiatives have occurred within the last few years, each of which serves to shape education and educational policy within Alberta. Each of these initiatives underline the importance of positioning school authorities with supporting digital citizenship policies. These provincial initiatives include extensive dialog and communications with Albertans through:

- *Inspiring Education: A Dialogue with Albertans (2010)*
- *Setting the Direction for Special Education in Alberta (2009)*

A brief overview of each of these initiatives is offered with a special view of the initiative through the lens of digital citizenship.

Inspiring Education: A Dialogue with Albertans

Inspiring Education takes a long-term, high-level view of education by exploring what Albertans will expect in a child's education in the year 2030, the year a child born today will come of age. The "three E's" of learning in the 21st Century are identified by Albertans as the qualities and abilities expected of youth:

Engaged Thinker: *who thinks critically and makes discoveries; who uses technology to learn, innovate, communicate and discover; who works with multiple perspectives and disciplines to identify problems and find the best solutions; who communicates these ideas to others; and who, as a life-long learner, adapts to change with an attitude of optimism and hope for the future.*

Ethical Citizen: *who builds relationships based on humility, fairness and open-mindedness; who demonstrates respect, empathy and compassion; and who through teamwork, collaboration and communication contributes fully to the community and the world.*

> ***Entrepreneurial Spirit:*** *who creates opportunities and achieves goals through hard work, perseverance and discipline; who strives for excellence and earns success; who explores ideas and challenges the status quo; who is competitive, adaptable and resilient; and who has the confidence to take risks and make bold decisions in the face of adversity. (Inspiring Education, 2010, p. 5-6)*

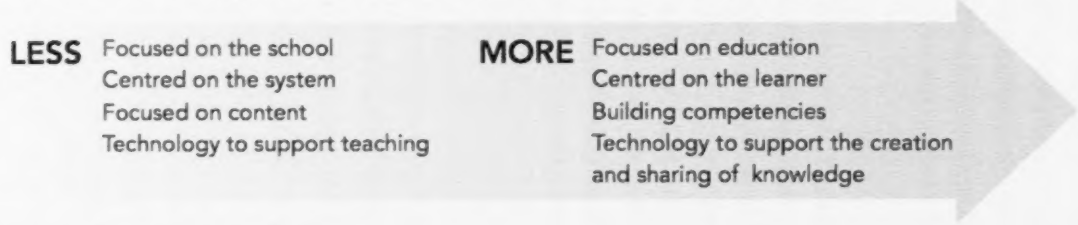
Importantly, within the three E's, Albertans identify both the role of technology in students' lives and the fundamental nature of preparing students as ethical citizens – significant elements in recognizing the important role of digital citizenship.

Further, one of the six core values underlying the three E's is citizenship. As an ethical citizen, the student of 2030 will value contribution, recognize their role as stewards of the earth, build meaningful relationships through teamwork, value diversity, display empathy and assume responsibility. These ethical citizens will "do the right thing because it is the right thing to do" (p. 19).

Inspiring Education also provides a strong sense of direction in the uses of technology in society and in the classroom. Within society, technology is anticipated to play a continued dominant role as shared by these points:

- *While natural resources will remain foundational to Alberta's economy, major advances in technology will impact how we access, develop and sustain our resource base.*
- *Some developing countries are bypassing the industrial economy and moving directly into a knowledge-based economy. The rate of change is accelerated by reforms in education and the availability of technology. Knowledge has become their new currency.*

Inspiring Education anticipates further change in Alberta's classrooms. The document points to the move toward more learner-centred learning and building of competencies with the use of technology supporting the creation and sharing of knowledge.



Further the document observes:

- Inspiring Education recognizes that technology community partnerships and post-secondary institutions can enable interactions between learners, experts, advisors

and mentors, wherever they may be. In so doing, Inspiring Education transforms the way we think about possible learning experiences and the way we address the learning needs of tomorrow. (p. 14)

- In community conversations, Albertans suggested using technology to connect schools with parents in their homes and workplaces. (p. 23)
- When community is truly an engaged partner in education, there can be "simultaneous participation in global classes taught by experts and enabled by technology." (p. 24)
- "As technology makes information instantly available, it is no longer possessed solely by experts." (p. 25)
- "Ultimately, the power of technology should be harnessed to support innovation and discovery, not simply to aid teaching. We need to engage learners to use these new technologies as designers and creators of knowledge." (p. 29)
- "A second, equally important role is assistive technology. This technology can help learners with special needs to more fully participate in learning activities." (p. 29)

Setting the Direction for Special Education in Alberta

Setting the Direction for Special Education in Alberta underlines the importance of an inclusive education system. In effect the document underlines the role of an ethical citizen through its vision:

> *One inclusive education system* where each student is successful.*
> **Inclusive education system: a way of thinking and acting that demonstrates universal acceptance of, and belonging for, all students. Inclusive education in Alberta means a value-based approach to accepting responsibility for all students. It also means that all students will have equitable opportunity to be included in the typical learning environment or program of choice.*

Legislative Alignment

Building upon the above initiatives, it is the intent of this guide to align with anticipated legislative changes that recognize the role of information technology in education and associated changes in the nature of support structures for students (e.g. the new Education Act).

Policy Insights

The backdrop of initiatives led by Alberta Education suggests changes in the nature of classrooms and teaching that is congruent with changes in society. A supporting vehicle necessary as such societal change continues is the need for policy change at the school authority level.

Defining Digital Citizenship

Digital citizenship brings forward a range of connotations. As a starting point, it is important to define the term. As a basis for thinking about digital citizenship, first consider the definition of citizenship.

> *Citizenship is defined as the state of being a citizen of a particular social, political or national community. Citizenship carries both rights and responsibilities.*

Within this definition, note three particular elements. First, citizenship occurs within a given community. Community is central to the definition. Second, for members of this community there are rights, such as the right to free speech. Finally, with these rights come responsibilities, boundaries within which community members must live.

In digital citizenship, this general framework still applies. However there are also some differences – especially at the level of specifics. Digital citizenship has its own set of nuanced rules that relate to citizenship, rules that are peculiar to the digital context. At some level, digital citizenship requires careful consideration.

Jason Ohler (2010) offers some important observations about this change in expectation and complexity. He shares his high school experience in traditional citizenship where Miss Phelps and Mrs. Hoover fully asserted their instructional responsibility of ensuring silence by striking fear into the hearts of students as they worked in the school library. To them, citizenship demonstrated recognition of the importance of proper behaviour within the context of the school library. Citizenship represented doing what was right and responsible within the given social context. Ohler continues:

> *Yet as we fast-forward to 2010, we wonder whether our notion of citizenship accurately reflects our needs. After all, a new perspective of citizenship has entered the public narrative that feels so different that we have given it its own name: digital citizenship. This term arises from the need to reconsider who we are in light of the globally connected infosphere in which we find ourselves. That is, given that citizenship seems to be directly related to behaviour and social organization, and given that the Digital Age facilitates new kinds of both, we need to update our perspectives about citizenship to provide a more complete picture of who we are.* (Ohler, 2010, p. 2)

Citizenship serves as a foundation and cornerstone for democratic nations. It provides the supports necessary to guide rights and responsibilities for civic engagement, for political engagement and for societal engagement. In essence, citizenship and now digital

citizenship, offer the underpinnings of a democratic society. Education serves as the fundamental vehicle to the continuance and shaping of this political and cultural ideal.

As noted by one Alberta superintendent of schools, "Digital citizenship will evolve just to citizenship. However, at this juncture there is a serious need to address the nuances of digital citizenship, to build capacity and to develop the necessary student and teacher knowledge."

The nature of citizenship as a basis for developing digital citizenship. Citizenship is defined as the state of being a citizen of a particular social, political or national community. While citizenship carries both rights and responsibilities, defining the particulars of those rights and responsibilities varies across time and across specific communities. Hence, a static and full generic definition is not a realizable goal. However, a fundamental goal in addressing citizenship and ultimately citizenship policy development, is encouraging conversations that engage the community. Such engagement operates within a framework that both describes citizenship and demonstrates some of its requirements. Ohler (2010) shares the nature of citizenship and requirements of citizenship, then contrasts these considerations with digital citizenship. Elements he has identified follow:

Citizenship requires working to high moral principles. Communities are composed of individuals – individuals who must work to make the community effective. Constituents of the community must be principled members to create an effective community. Digital citizenship similarly requires moral principles to effectively work within online, time-separated and geographically independent, multi-cultural, global communities.

Citizenship requires balancing personal empowerment and responsibility with community well-being. The good of the individual and the good of the community must reside in a state of equilibrium. The challenge within digital communities is ensuring an effective balance. Individual members can affect unforeseen outcomes upon the community and other individuals. These effects are often not obvious, given geographic and time independence.

Citizenship requires participation. Communities, whether local, regional, national, social or political require members to participate for the community to have value and meaning. Without participation the community becomes non-existent. Digital communities similarly require participation and society has a role to play in preparing youth to participate in these communities in meaningful, responsible and caring ways.

Citizenship requires education. Attaining high moral principles in community interactions does not occur automatically. It requires guidance, typically from an elder's (e.g. teacher's) hand. Education in digital citizenship has even greater need and often is even more challenging to guide, given its sometimes abstract nature.

Citizenship is ever-evolving and thus requires ongoing conversation and debate. What is appropriate in one time-frame or culture is not necessarily appropriate in the next. Digital citizenship, as a relatively new form of citizenship, will require ample conversation – especially as society works to educate youth in this new realm.

Citizenship must be inclusive. Society cannot afford to regress to earlier historical models where one culture or community had greater citizenship rights than others. Digital citizenship is further shrinking the globe, creating new relationships, meaning and communications. Equality and equity will need to be watchwords in this new citizenship form. This is particularly tricky in Kindergarten to Grade 12 education settings where a sliding scale of responsibility and associated rights are necessary based upon a child's readiness and development.

Citizenship has close linkage with media advancement. Changes in media have resulted in changes of community and community relationships. Digital communities are only possible through media forms that have enabled their creation.

Finally, citizenship is intimately tied to community. Citizenship does not reside in a vacuum – it must have a community. Digital citizenship has reformulated the reach and nature of communities. Such communities can now be multi-cultural, global, highly-focused and long-tailed (Anderson, 2006). Educators need to decide if they are prepared to guide students in learning to meaningfully engage such communities.

The term *digital citizenship* creates a new form of citizenship. While it builds upon the concepts of citizenship, subtle characteristics and nuances are part of this newer form. The nature of these specific characteristics is shared later in this guide.

The Need for Digital Citizenship Policy

Multiple factors lead to the importance of establishing digital citizenship (Appendix A). The global context suggests significant changes in society and work, largely due to ubiquitous pervasively-connected mobile technologies. The provincial context reflects the need for change through such initiatives as Inspiring Education, the College of Alberta School Superintendents' (CASS) 12th Dimension of the Framework for School System Success, a breadth of research activities (including the Emerge One-to-One Laptop Learning initiative) and the provision of support infrastructure through the Alberta SuperNet. These elements align with formative legislative policy discussions as found within the proposed Education Act.

Within this context, Alberta students are employing mobile technologies, frequently independent of schools, for social and entertainment purposes rather than educational intent. As Ohler (2010) asks:

> *Should we consider students to have two separate lives—a relatively digitally unplugged life at school and a digitally saturated life away from school—or should we consider them to have one life that integrates their lives as students and digital citizens?*
>
> ...
>
> *The "two lives" perspective says that ... kids will have to figure out how to navigate the digital world beyond school on their own and puzzle through issues of cybersafety, technological responsibility and digital citizenship without the help of the educational system.*

A division of lives has left students technically able to project significant power, yet lacking the supporting structures to guide ethical development.

This division of lives has left students technically able to project significant power, yet lacking the supporting structures to guide ethical development. James et al's (2009) research indicates that youth are often confused by the power of the new technologies where they may easily conduct activities, such as download music, copy text or images and duplicate software, that are ethically questionable and technically illegal.

Harvard University's GoodPlay Project (2009) found through a series of focus dialogues that:

- Teens are most likely to engage in individualistic thinking with concerns for self across such topics as sharing information online, illegal downloading and cyberbullying.
- Teens are somewhat likely to engage in moral thinking (concern for others).
- Teens are least likely to engage in ethical thinking (thinking in abstract terms about the effects of one's actions on the online community).
- Adults, on the other hand, show much stronger and consistent patterns of moral and ethical thinking about digital dilemmas – suggesting a need for adults to provide guidance and lead youth as developing digital citizens.

In addition to guidance, student safety must be of concern to both parents and educators given frequent use of highly mobile digital technologies. Leadership advisement (CASS Conference Communication, November 4, 2011) indicates school authorities hold increasing responsibility for student behaviour - particularly behaviour beyond the school yard.

In addition to guiding schools, digital citizenship policy can also provide direction for teachers and school authorities. Educators are often seeking direction in their use of

contemporary technologies for both professional and personal use. Organizations often struggle with the nature of communications in an open, non-hierarchic and often anonymous context. Digital citizenship policies can guide school authorities and educators with these challenges.

Importantly, the process associated with establishing a digital citizenship policy can offer a valued stepping-stone in addressing student learning needs. In working to build an effective balance between open-access to information and communications to enable student learning and the need for addressing potential student-risk, fundamental conversations may be hosted with stakeholders that examine the values and the culture held within the school authority. Ultimately from these conversations can spring philosophic underpinnings, policy, regulations and guidelines that will serve student learning and help organizations in building a framework to support students' knowledge of digital citizenship and address numerous contemporary challenges in this domain.

> ...***process*** of policy development to address digital citizenship is much more important than the ***product***.

Compliance or Commitment

As shared by senior leaders who have demonstrated success in digital citizenship policy development, the ***process*** of policy development to address digital citizenship was much more important than the ***product***. Conversations supporting the development of specific policies were fundamental to the organization. While a policy statement taken from an exemplar may serve some role, from a broad leadership standpoint it will likely fail to serve the organization. Stakeholders would be required to comply with given policies that may or may not fit their context and for which they feel has little salience or relevance.

As shared by Lencioni (2002), leading by expecting compliance is largely an ineffective approach to leadership. Significantly stronger leadership strategies demonstrate the importance of 'process' in achieving outcomes (e.g. Collins, 2001; Fullan, 2003; Fullan, 2001).

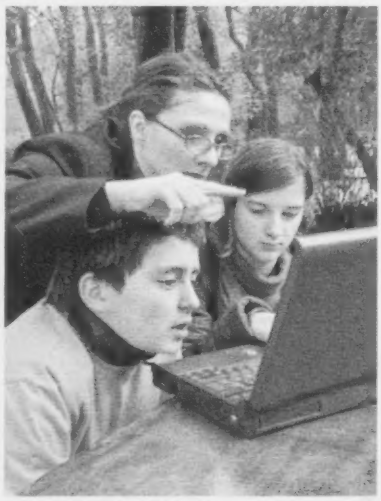
> Stakeholders participating in the process of policy development are more likely to feel a sense of commitment to digital citizenship policies developed through meaningful involvement.

By focusing upon the process of policy development, a shift to 'commitment' occurs. Stakeholders participating in the process of policy development are more likely to feel a sense of commitment – to digital citizenship policies developed through meaningful involvement. Commitment on behalf of stakeholders provides a) insights and perspectives from a breadth of stakeholders; b) a process for stakeholder collaboration and involvement; c) opportunity for stakeholders to educate

themselves and others on digital citizenship and associated policies; d) an improved set of policies that better address the specific context within the organization; and e) a means for developing deeper policy layers (e.g. administrative procedures and guidelines).

Given the recognition of the importance of community, organizational culture and stakeholder involvement, this guide will define the broad context of digital policy development and provide a suggested process for developing digital citizenship policy.

The end goal is to realize stakeholder commitment to the process and to outcomes effectively addressing digital citizenship, rather than simply seeking compliance.



2. Method

Research Methods

This work is based upon three research sources. First an extensive literature review was conducted, consisting of both formalized literature (peer-reviewed research, dissertations, organizational research and published books) and informal literature (blogs, wikis and websites). This review examined the nature of citizenship, the nature of digital citizenship, current digital policies and contemporary digital successes and challenges in schools.

Second, numerous interviews were conducted with leaders from across Alberta. Perspectives and information was gathered from senior leaders and other educators to help shape this work. Formal interviews were conducted directly and via teleconference with superintendency leaders and committees representing a broad range of locations, school authority size and demographics. These leaders, recognized within the Acknowledgements section, generously shared their time and expertise. These insights helped shape this guide. As well, the College of Alberta School Superintendents (CASS) hosted a session at its 2011 Annual Conference where feedback from leaders was gathered.

Finally, a blog served to gather further insight and feedback from educators. This blog can be found at SpeakingofITLeadership.com. Continued conversations are welcomed.

The interviews, conversations and feedback shared through the SpeakingofITLeadership blog have been critical in shaping this work.

3. Understanding Digital Citizenship

At its base, digital citizenship is rooted in traditional citizenship. The underlying values of citizenship serve to inform and guide digital citizenship. However, digital citizenship details a new dimension of citizenship. It presents nuances and considerations that are complex in nature.

Some of these nuances are captured within the International Society for Technology in Education's (ISTE) National Education Technology Standards (NETS). NETS describe performance indicators for three different roles: students, teachers and administrators. A complete listing of the digital citizenship elements from student, teacher and administrator NETS are provided in Appendix B. These indicators, which support digital citizenship policy, include:

- Educational administrators will promote, model and establish policies for safe, legal and ethical use of digital information and technology.
- Teachers will develop and model cultural understanding and global awareness by engaging with colleagues and students of other cultures using digital-age communication and collaboration tools.
- Students will demonstrate personal responsibility for lifelong learning.

An example of an AUP policy might include statements such as:
The following kinds of behaviours shall be considered inappropriate use of electronic information learning resources:

- *Intentionally retrieving or displaying offensive messages or graphics;*
- *Using obscene language;*
- *Gaining access to, or participating in, electronic chat lines;*
- *Damaging computers, computer systems or computer networks.*

Acceptable Use Policies Relative to Digital Citizenship Policies

A clear distinction between acceptable use policies (AUP) and digital citizenship policies must be drawn. This distinction is important in helping one think about the nature of these policies. The difference between acceptable use policies and digital citizenship policies may best be

summed up by media scholar Henry Jenkins: "Kids don't need us watching over their shoulders; they need us to have their backs." (ZDNet, 2007). A closer look at each policy type is in order.

Acceptable Use Policies

Acceptable use policies tend to emphasize the problems, issues or challenges especially relating to behaviour. The focus is frequently on student behaviour, or more specifically, control of behaviour. Importantly, these policies tend to assume that digital access is not a fundamental learning tool.

Sometimes the term "responsible use" replaces the term acceptable use. Some school authorities have explored reframing their acceptable use policy with responsible use, sometimes signaling greater liberalization of expectations and deeper associated responsibilities. Acceptable use and responsible use policies tend to be less comprehensive than the expectations associated with digital citizenship policies.

Digital Citizenship Policies

Digital citizenship policies tend to focus on student learning and student needs. Rather than attempting to control student behaviour as found in acceptable use policies, the emphasis is on how to teach students to work, live and share in digital environments. A fundamental assumption is that students will be using online technologies as part of learning to prepare for life in a globalized connected society.

While this distinction between acceptable use and digital citizenship policies is helpful, it is also noteworthy that elements of each have some value. AUPs clearly delineate the rules, helping learners and educators understand the boundaries. Digital citizenship policies value learning and recognize the critical role that technologies play in learning for today's student.

Digital citizenship policies may include such statements as: *The Master Learner School Division supports opportunities for student collaboration, problem-solving and personalized learning through contemporary information technologies supporting learning environments. The district uses such technology to facilitate innovation and creativity. Within this spirit students will show commitment to the following values:*

- *Respect Myself. I will select online names that are appropriate, I will consider the goodness of information and images that I post online.*
- *Respect Others. I will not use technologies to bully or tease other people.*

Digital Citizenship Policy: A Foundation for Digital Citizenship Instruction

Digital citizenship policies serve as a foundation to support and guide digital citizenship instruction. While digital citizenship instruction is not currently formalized curricula, sections addressing digital and technological fluency are within the *Framework for Student Learning: Competencies for Engaged Thinkers and Ethical Citizens with an Entrepreneurial Spirit* (Alberta Education, 2012b). The intricate relationships within this model are shared through a conceptual model as shown in Figure 1. To enable digital citizenship, parameters and direction, as found within digital citizenship policy, are needed.

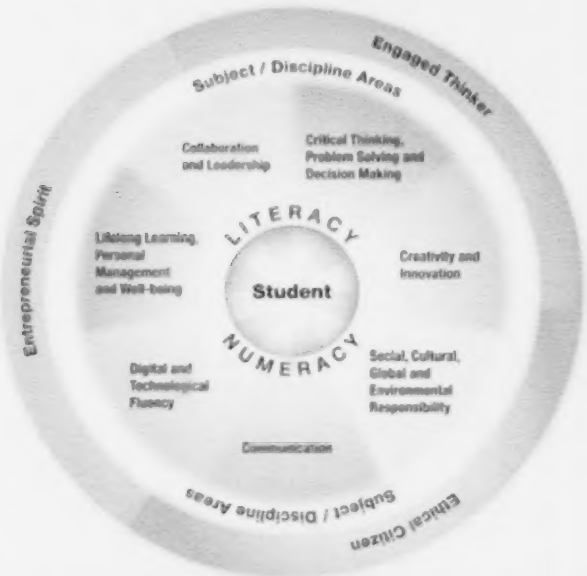


Figure 1. A conceptual model for the Framework for Student Learning.

Policy Insights

Both digital citizenship and acceptable use policies are needed to provide direction, education and supports as well as clear parameters for personnel and students. Acceptable use policies may need to be updated, but they continue to serve a role in identifying clear direction. Digital citizenship policies serve the important role of preparing students and organizations for a changed and changing society.

4. A Digital Citizenship Policy Framework

At its most elemental level, digital citizenship encompasses the following facets, as shared by Andrew Churches:

Respect

- Respect Yourself
- Respect Others
- Respect Intellectual Property and Other Property

Protect

- Protect Yourself
- Protect Others
- Protect Intellectual Property and Other Property

While this overview helps when thinking about the basic elements of digital citizenship, a more comprehensive consideration is required in a school authority policy context. A more detailed structure is offered through Ribble's (2011) research:

1. Digital Access: Full electronic participation.
2. Digital Commerce: Online buying and selling of goods.
3. Digital Communications: Electronic exchange of information.
4. Digital Literacy: Process of teaching and learning about technology and the use of technology.
5. Digital Etiquette: Standards of conduct or procedures online.
6. Digital Law: Responsibility for actions and deeds using electronics.
7. Digital Security: Electronic precautions to protect learners, staff and organizations
8. Digital Health and Wellness: Physical and psychological well-being in a digital world.
9. Digital Rights and Responsibilities: Freedoms extended to those in a digital world.

This framework will be appended to include contemporary digital citizenship policy issues. Additional issues of relevance include cloud computing and personally owned devices.

In keeping with Ribble's (2011) work and also in keeping with literature in the field, some of the elements within the framework receive extensive description, whereas other elements are much more abbreviated. This is reflected in the literature where elements such as digital communications serve as a focal point for strategic planning (e.g. Kay & Greenhill (2013)) or are central to curricula (e.g. English Language Arts), or are fundamental to the

nature of contemporary technologies (e.g. Web 2.0 communications). Other categories such as digital commerce, while important, hold a less fundamental role and remain thus represented.

From a policy and implementation standpoint, it will likely be helpful for school authorities to identify priorities across these elements. Which of these elements should become policy in the immediate future (say, the current year)? Which should become policy in the next two to three years, and which should have a longer-term policy resolution?

Digital Citizenship Policy: Nine Elements

The following sections use Ribble's nine elements of digital citizenship as a framework for thinking through the key digital citizenship policy areas. The format followed within each of the nine framework elements includes a) a description of the element itself with relevant research and detail; b) policy considerations, which consist of questions one should consider during policy development; and c) policy questions, which consists of questions that are either required by law or highly recommended for discussion during policy development.

1. Digital Access

Digital access refers to "full electronic participation in society" (Ribble, 2011). Information technology provides a platform that connects learners with a world-wide library of information and, importantly, with other learners, educators and people who can contribute significantly to their education and development.

Although schools have been purchasing technologies for many years, ready access to Internet-connected technologies is not necessarily available to students at the time of learning need. Student-to-computer ratios are much improved over earlier times, but ready access is not always possible. This is changing as students increasingly carry their own digital devices. Such devices will continue to become more and more commonplace in students' hands. Schools will need to decide their role in preparing students for a digital future. As part of this decision, they will need to determine student access using personal devices within educational contexts (Alberta Education, 2012a).

Access to the digital world for some students is limited due to the nature of available interfaces. For example, students with severe visual impairments or auditory impairments may require a specific interface such as speech input or speech synthesis. Opportunities for digital

The United Nations (May 2011, A/HRC/17/27) called for rights to the Internet as a basic human right. Two access rights were noted:
a) the right to access online content without blocking restrictions (except in limited cases under international human rights law, e.g. child pornography); and
b) the right to access infrastructure and information communications technologies in the form of computers, software and networks.

access are easier than ever before, but such opportunity has reliance on policy decisions. Systems tailored to individual learner needs are increasingly available. Decisions on access for students with specific needs, as well as general needs, are coming to the fore. Decisions should include consideration of access to personally owned devices, to the Internet, to content, to specialized interfaces and to school authority digital networking infrastructure.

Policy Considerations

- Has your school authority thought about its role in supporting or not supporting personally owned devices?
- Does your school authority have the capacity to teach digital citizenship or does it need to provide professional development avenues to address it?
- Is your school authority blocking content? If so, are educational staff involved in the blocking decisions? Is your school authority satisfied that such blocking serves student learning?
- Does your school authority envision moving away from content blocking and onto digital citizenship education over the long-term?

Policy Questions

- Does your school authority's policy offer a philosophic statement recognizing the fundamental role of pervasive connectedness and its influence on students and student learning?
- To enable meaningful access, does your school authority's policy support equitable levels of student access, including students with specialized needs and students from low socio-economic groups?
- Does your policy encourage students to use their personally owned digital devices within your school authority? If so, has your school authority provided policy parameters guiding the use of personally owned devices?

2. Digital Commerce

Students spend significant personal funds across the Internet. According to Harris Interactive (2003), young adults aged 8 to 21 years spend approximately $172 billion per year. Of that amount $25 billion is spent online.

In spite of such activity levels, there are security considerations that students frequently misunderstand or overlook. For example, boyd [sic] (2010) reports students sharing passwords with friends as a statement of kinship. Livingstone & Haddon's (2011) research shows that 7% of 11 to 16 year olds have had others use their password and 1% of this age group has lost money to being cheated on the Internet. While 1% does sound somewhat

insignificant, by extrapolation this would amount to $250 million in theft, based upon the above $25 billion annual expenditures.

Policy Considerations

- Has your school authority examined its role in preparing students in digital commerce (e.g. to protect themselves from identity theft and Internet purchasing scams)?
- Has your school authority thought about whether it encourages or discourages the use of school authority resources for student commercial endeavours, for class commercial endeavours or for educator commercial endeavours?
- Has your school authority thought about occasions where students or educators are on a school authority campus, but using their own device and their own network for commercial purposes or for volunteer fund-raising purposes?

Policy Questions

- What is your school authority's policy with regard to using school authority resources (e.g. network) to purchase school authority and/or personal items online?
- Are students in your school authority well-versed in the risks and opportunities associated with purchasing or commercial transactions across the Internet?

3. Digital Communications

Communications have changed dramatically across the past two decades. Social networking, Web 2.0, cell phones and texting have all changed the ways societies and students communicate. Students communicate as easily with others around the globe as next door. Schools have struggled with this new dynamic, and currently there is a breadth of policies and approaches to digital communications in schools and classrooms. Some see learning opportunities and embrace such communications changes; others cautiously do not permit the use of contemporary communications tools in the classroom or school.

Educators must have conversations about the role of today's communication tools in our educational settings and seek a meaningful balance in this domain. There are several necessary conversations including: the learning environment, pedagogical approaches, student safety, privacy, global responsibility, identity management and information security – all in the interest of preparing students as digital citizens.

Digital Communications – Considerations and Challenges

Students are able to express themselves to their local classmates and to global audiences in ways never before envisioned. Not only are the potential audiences expanded, but the nature of possible creative expression is also expanded. Text, voice, audio, images and movie clips are all easily within the realm of student expression and creativity.

Asynchronous communications enable the user to communicate or receive communications independent of time. Such communications become a digital record that is maintained and consequently persists across time. This persistence can serve learning as students record insights, share and collaborate. This same persistence can also cause harm to students.

As these communications are typically world-wide, some policy considerations may be desired to distinguish between personal representation and employee/student representation. It may be helpful for employees to give consideration as to whether they are speaking on behalf of themselves, their class, the school or the school authority and whether they have rights to provide such perspective.

Synchronous communications, on the other hand, such as texting or chat services, requires the immediate attention of the communicator. Such communications often have a sense of immediacy, but are not typically on digital record. Such communications can increase feedback from students to teachers and increase home to school communications, but it can also prove to be a distraction.

Inappropriate use can occur across either asynchronous or synchronous mediums. Synchronous texting via a cell phone during class time is disruptive of the learning environment; beyond poor digital etiquette, such behaviour imposes upon the learning of all class members. Asynchronous messages of an inappropriate nature posted to a blog can quietly create significant disruption for an individual or for a class as a whole. Both communication forms present significant learning opportunities and digital citizenship needs.

Identity:

As youth communicate, create and collaborate in online digital realms – whether on their own or within school contexts – they are progressively building a digital identity. This identity will remain public across many years – whether positive or negative and whether posted from home or from school. Education can have significant value in guiding youth to build digital identities that serve them and are valuable to their future.

While digital media may benefit identify formation, the types of self-expression, self-reflection and feedback conducted online may undermine identity formation for some learners struggling with a myriad of social roles without a sense of coherency and

responsibility. A guiding hand from educators can assist learners in digital identity development, much as the same guiding hand can assist learners in offline identity development. The key challenge is educator involvement and knowledge in the digital citizenship arena.

Privacy:

In keeping with considerations of building an online identity are also considerations of privacy. In his book, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Solove (2007) presents a compelling argument that the nature of privacy is changing and that any act in public risks becoming a part of the Internet's digital archive, a permanent ongoing record of the act – whether positive or negative.

boyd [sic] (2008), in her extensive ethnographic research on practices of teenagers using social media, references three dynamics affecting youths' experiences in public networks and affecting the nature of privacy: a blurring of public and private practices, producing information for invisible audiences and collapsed contexts wherein the lack of spatial, social and temporal boundaries makes it difficult to maintain distinct social contexts.

boyd's (2010) work suggest a dramatic change in youths' interest in sharing across a public setting. Once material is published, the nature of the Internet has bearing on the privacy of information through four properties:

- Persistence (what is posted remains indefinitely);
- Searchability (easy to find using common search terms);
- Replicability (one can copy and paste the information into new contexts); and
- Invisible audiences (there is minimal control over public and private messaging/sharing).

Each of these contributes to a change in the nature of privacy. As well, each also underlines the importance of digital citizenship and discussions regarding varying perspectives and mores in a digital world.

Classrooms are potentially less private than ever previous. Progressive educators openly share insights and activities in their classrooms (Fisher, 2011; Branigan-Pipe, 2011; Wright, 2011). Perceptions of instruction and schools can be rated and openly shared through today's Web 2.0 tools. While policy is not a vehicle to control student discussion, policy development can be used to create open meaningful dialog within school authorities and schools on communication issues.

Policy Considerations

- In your school authority, what guidance are students receiving in appropriate communications? Are there clear expectations for public communications through Web 2.0 and social media? Are the parameters clear?
- In your school authority, what educational guidance are students receiving in developing their digital identities?
- In your school authority, are students and educators participating in educational conversations about the nature of privacy and public sharing? Are students guided in what they can share publicly and what must remain private (e.g. limits of personal information, photos, video)?
- Has your school authority given consideration to the management of inappropriate public expression by students? By staff? By parents? By community?
- Has your school authority provided guidelines to support students and educators in appropriate communications?

Policy Questions

- Has your school authority policy addressed online bullying either as part of a bullying policy or as a separate policy item?
- What policies provide guidance for students and employees as they represent your school authority or school in a publicly-viewable online context?
- Has your school authority provided guidance to help employees and students understand the parameters of representing themselves versus their school versus the school authority?

Digital Communications – Managing Content and Communications

When working in a digital environment, there is sometimes a need to distinguish between information actively sought and information passively received. This distinction is helpful whether considering an active search using a search engine, postings on a Web 2.0 site or social media site, text messages, Twitter exchanges or e-mail received. In developing policy, this distinction can prove helpful.

Most school authorities have long maintained some degree of control over information sought on the Internet. While content management systems are far from perfect - sometimes blocking that which should be accessible and sometimes missing that which should be blocked - they have provided a degree of control.

However, there is increasing recognition that content management is a stop-gap measure offered within the narrow context of using school-owned digital devices during school hours. Students frequently use unfiltered Internet outside of school. Given the recognition that content management does not prepare students for outside the school context, given

challenges with content control categories and given the ongoing costs, some school authorities are exploring a long-term strategy of removing content management and instead focusing their energies on effective digital citizenship strategies.

This strategy also recognizes the ever-increasing role of communications via the Internet. In a Web 2.0 context, communicating with strangers is frequently the norm, as unknown individuals post to a Web 2.0 site. Generally speaking, such posted communications can prove educationally valuable. However, the ever-present fear among adults is that connection between a student and an online stranger leads to harm. Research from EU Kidsonline (Livingstone & Haddon, 2011) indicates that while there is a tension between how children view "making new friends" and what adults consider "meeting strangers," the greatest fear from a student's perspective is, instead, peer-to-peer contact in the form of bullying. Policy can guide students and educators in assisting students to safely interact with others not immediately known.

Policy Considerations

- Has your school authority considered enabling communication with the outside world on a sliding scale across grade levels? A combination of technical approaches and digital citizenship instruction can serve to provide as open a communications system as possible and best ensure student safety.
- Do policies balance the need for personally owned devices with educational value that can be gained from these devices?
- Has your school authority provided guidance for employees and students in the receipt and handling of inappropriate communications (e.g. texts, e-mail, Web 2.0 postings)?

Policy Questions

- How has your school authority accommodated and balanced the educational value of student-owned devices with the need for a learning-focused school environment? Is there digital citizenship policy and instruction within the school authority to enable this combination?
- What plans are in place to ensure that students with high needs have high levels of access to online communications and information?
- What policies will need to be in place as schools are pushed toward making content management changes? Is there a transition plan to reduce blocking or remove blocking? Does your school authority's digital citizenship instructional plan align with this plan?

4. Digital Literacy

Introductory skills and development of technical skills by students does not equate to deep understanding of appropriate use of digital technologies. boyd's extensive research (2009) suggests that media literacy among networked teens is extremely varied and that they have virtually no media literacy training.

Even introductory level skills are not necessarily strong among students. Livingstone & Haddon's (2011) research indicates:

- Only 36% of children aged 9 to 16 perceived that it was *very true* that they knew more about the Internet than their parents;
- 66% of children aged 9 to 10 say it is *not true* that they know more about the Internet than their parents;
- 37% of students did not have the skills associated with finding safety information online;
- 36% of students were unable to bookmark a website;
- Nearly 50% could not change privacy settings on a social networking profile; and
- Over 50% were unable to block spam.

As noted by Livingstone & Haddon, "Talk of digital natives obscures children's need for support in developing digital skills" (p. 42).

Ribble (2011) points out the importance of students understanding the specifics of digital tools, but also points out that students must have opportunity for this tool set to be part of the school's curriculum to explore how it may be used appropriately. A significant element in this picture is the development of teachers' abilities in using technology and how to plan and engage students using meaningful digital technologies in appropriate ways.

Policy Considerations

- Does your school authority provide online course offerings and courses that are a blend of face-to-face and online components?

Policy Questions

- What expectations exist for educators and students to develop digital literacy that addresses digital tool skills, classroom infusion and discussions of appropriate and inappropriate uses of technology?

- How does your school authority support educators in their quest for knowledge of both digital tool skills (how do I use...) and pedagogical change (how do I apply those tool skills in my classroom)?

5. Digital Etiquette

Digital etiquette refers to the standards of conduct expected within digital contexts. Comparing it to a sense of etiquette in the physical world, one will find parallels. However, there are also some significant differences. There are relatively long-standing standards for behaviour in the physical world; change has been so rapid and dramatic in the digital world that everyone is adapting. Parents, who once took primary responsibility for etiquette instruction, often no longer have the knowledge or participation levels to guide or model etiquette in the digital context. Students, who frequently have substantive experiences in digital contexts, have their own sense of etiquette behaviour in these contexts relative to adults.

Continuing this comparison, the physical world typically presents a context that encompasses recognizing people, their roles, their stature, the specific environment (e.g. a friend's house versus a formal social event) and other similar cues which guide etiquette (e.g. addressing a friend versus a policeman). The digital world similarly has context, but the associated cues are quite different and the sensitivities may need attention.

For example, when publishing in a Web 2.0 context, one will only know that the potential audience is large and varied. One may not know anything of participants' roles, stature or their environment. One may be publishing anonymously to an audience that is likely multi-cultural. While the choice of digital tool may provide a rough gauge, spatial and temporal signals do not exist. These cues and the lack of cues hold a degree of bearing on etiquette.

A distinguishing feature of digital etiquette, relative to physical world etiquette, is that in the physical context educators frequently have opportunities to guide student etiquette and deportment. Much of the interaction within a digital context remains private, especially given mobile devices. Only through effort and explicit guidance can educators achieve parallel reach in digital etiquette instruction.

Policy Considerations

- What is your school authority's approach to guiding student digital etiquette, given the rather private nature of online communications?
- What is your school authority's approach to guiding employee digital etiquette in these new contexts?

Policy Questions

- What is your school authority's policy with regard to accessing communications (e.g. e-mail, non-public cloud-resources)?
- Should your school authority have the right to access student communications? Employee communications? (Note: This has relevance to digital etiquette, student safety and digital law.)

6. Digital Law

Digital law refers to legal requirements, legal decisions and ethics that relate to digital environments. Digital law can directly affect students in classrooms, employees and organizations as a whole. Some of the legal developments in Canadian law have proven evolutionary. As Horton and Thomson (2008) note in their description of Canadian law, Canada has chosen to emphasize and promote self-regulation over extensive legislation. Public awareness and education have been the tools chosen to promote child and family safety. The authors observe that the Canadian approach to legislative references may be summed up as, "If it is illegal offline, it is illegal online" (p. 63).

Canadian digital law is largely reliant upon existing law, rather than specialized laws. However, given that many Internet services used by Canadians are based in the United States, U.S. law does have some relevance.

While this section will not presume to provide an all-inclusive list of legal considerations and does not provide legal advice (please seek professional legal advice on all legal matters), it does provide a number of considerations for leaders in developing policy.

Student and Educator Considerations

Educators and students may inadvertently, or intentionally, break laws through digital means. As well, external persons or organizations, outside the school, the school authority and potentially in geographically distant locations, may break the law through digital means, affecting students, personnel or the school authority.

Looking at legal concerns within the school authority, plagiarism is of particular interest to many educators. This is largely rooted in the ease with which information can be copied and pasted from other sources without recognizing the original source. While the base of the concern is frequently rooted in traditional text-based plagiarism, the possibilities include a variety of media (e.g. audio, video, photographs, graphics). As well, the nuances associated with authorship and ownership can prove less clearly defined in a digital context.

The term *mashups* begins to demonstrate more complex requirements for defining the term 'plagiarism' and dividing lines between appropriate and inappropriate use. Ownership of

material is much less clear when a breadth of media is aggregated into a mashup – sometimes to the point where any one of the originals is not readily identifiable.

Even traditional text-based copying and pasting presents new and unforeseen nuances in the electronic world of digital citizenship. The vignette below, "Digital Citizenship and Authorship," shares some of these nuances.

> Wikipedia: a mashup is digital media content containing any or all of text, graphics, audio, video and animation drawn from pre-existing sources, to create a new derivative work.

Canadian law clearly supports copyright ownership and respect of intellectual property. Recent amendments to the *Copyright Act* were passed in 2012 that address the nature of the Internet and how it enables copyright infringement. The amendments address activities such as the downloading of copyright protected material, such as music and videos. This presents considerations for education in instructing students about legal expectations and possibly limiting opportunity for such behaviour in school contexts.

It is noteworthy that there appears to be a different sense of ownership rights between students and adults. Based on an Ipsos research poll (Ribble, 2011, p. 31), significantly more faculty and administrators (approximately 66%) than students (approximately 25%) indicated it was wrong to download or swap files. Clearly, the sense of copyright and ownership rights is not a strongly held value, particularly among students and particularly in an era when the boundaries are more highly nuanced. Digital citizenship policies should recognize the legal requirements associated with the *Copyright Act* and accommodate the more nuanced domain of Internet collaboration, sharing and mashups within this legal requirement.

Legal considerations for students do not end at the potential for plagiarism. Other legal considerations policy developers should review include:

- Identity theft;
- Software or music theft (piracy);
- Computer hacking or harm (e.g. virus development);
- Failure to protect confidential digital information (e.g. unencrypted data, data storage or movement, lack of protective networking structure, lack of appropriate server architecture); and
- Failure to indicate ownership and rights to access data (e.g. rights to school authority-owned e-mails, rights to access Web 2.0 resources owned by staff and students as part of school authority work).

Vignette: Digital Citizenship and Authorship

Based upon work from James et al (2009), the following fictionalized vignette captures the nuanced changes in our conception of digital citizenship and authorship.

> Daniel is a Grade 11 student who is interested in social movements and occasionally contributes articles to Wikipedia, the online encyclopedia. When he is given the chance to write a research paper about the Occupy Movement for a Social Studies class, he decides to compare the effectiveness of rallies that occurred across Canada in 2011. In his paper, he draws extensively from a Wikipedia entry about the Occupy Movement to which he contributed a few months earlier. After reading Daniel's paper, his teacher calls him into her office and accuses him of plagiarism, noting that he used verbatim lines from Wikipedia without giving proper credit to the source. Daniel replies that since he was the contributor to the Wikipedia article, his use does not constitute plagiarism. He also argues that the passages he used were mainly historical supporting facts and that the core of the paper is his unique analysis of the movement's significance as a protest movement. Above all, he asserts, the purpose of Wikipedia is to make knowledge available for widespread use. It does not provide the names of article authors and he will not be cited by others for his contributions. In fact, authorship is irrelevant.
>
> *Permission for the above granted: Original concept provided by James et al (2009) in Young People, Ethics and the New Digital Media: A Synthesis of the GoodPlay Project (p.45) – supported by the John D. and Catherine T. MacArthur Foundation.*

Organizational Requirements: Bullying and *Freedom of Information and Protection of Privacy Act*

Some existing legislation is clear with regard to school authorities' requirements and subsequent digital expectations. However other legislative areas remain less clear. For example, the provincial *School Act* indicates board responsibility for student protection, but does not address online bullying. Given the nature of online bullying and given extensive legislative policy discussions, it is recommended that policy also clearly address cyberbullying. Unlike traditional bullying, online behaviours present new pressures on the bully's target in the form of anywhere/anytime access, permanence once posted on the Internet and access by a global audience – all without a sense of who has participated or observed the bullying incident.

Some aspects of the Alberta *Freedom of Information and Protection of Privacy Act* (FOIP) also present a challenge. Over the past decade, rights to information access quickly became of concern as technological advances enabled rapid movement of information, sometimes consisting of confidential sources. As a result FOIP legislation, governing the sharing and access to information, was passed.

Within a digital context, technical subtleties can sometimes obscure the risk of illegal access to information under FOIP legislation. Consider the following example where legislation may come into effect in the case of cloud computing storage of data. FOIP legislation indicates:

> *Section 92 (3) A person must not willfully disclose personal information to which this Act applies pursuant to a subpoena, warrant or order issued or made by a court, person or body having no jurisdiction in Alberta to compel the production of information or pursuant to a rule of court that is not binding in Alberta.*
> *(4) A person who contravenes subsection (3) is guilty of an offence and liable*
> *(a) in the case of an individual, to a fine of not less than $2000 and not more than $10 000, and*
> *(b) in the case of any other person, to a fine of not less than $200 000 and not more than $500 000…*
> (Queens Printer, 2009)

This legislation could be relevant when servers reside within the United States and the data stored is personal data (e.g. private personnel or student information). The United States' *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, more commonly known as the USA Patriot Act, provides enhanced surveillance measures (Title II) that enable access to data in transmission or in storage within the United States. This act entitles American citizens in authority under this act to access files, independent of their origin – thus potentially contravening the intention of FOIP legislation. This suggests caution with regard to storing personal information "in the cloud" (e.g. student information systems data, payroll records or human resource records) and further suggests researching where servers reside.

Organizational Requirements: Policy Specificity

It is recommended that school authorities include specific expectations within policy as this can affect litigious outcomes. A lengthy and detailed court proceeding heard before the Supreme Court of Canada exemplifies this need. Details of this court proceeding are shared in the vignette "Ontario Legal Case." While no legal opinion will be offered here, there is a need to be explicit in terms of expectations when developing policy related to digital citizenship. *Canadian Employment and Pension Law* (2011) underlines this recommendation:

> *As such, it remains prudent for employers to implement properly drafted internet and electronic use policies, particularly regarding electronic devices.* (*Canadian Employment and Pension Law*, 2011)

Vignette: Ontario Legal Case

In an Ontario legal case (Ontario Court of Appeals, 2011), the defendant, a high-school teacher, was charged with possession of child pornography, which was found on a school authority-owned computer operated by the defendant.

In the due course of his work, a technician found child pornography on the computer and turned the matter over to the principal, who, in-turn, contacted police. At issue was whether the teacher had reasonable expectation of privacy regarding the contents of the computer where the pornographic materials were stored. In the ensuing court proceedings, the trial judge determined that the teacher's privacy rights under the Charter of Rights had been infringed upon, thus excluding evidence found on the computer. Two other appeals ensued, with the final appeal accepting evidence and giving due consideration to privacy rights. Within such consideration, the Ontario Court of Appeals (2011) noted the school authority's policy and associated wording:

> *[17] A Policy and Procedures Manual, prepared by the school board for all of its teachers, permitted personal use of the computer. The policy provided there was to be no inappropriate content on the school computer, including sexually explicit material. Section P9.06 of the policy provided that "all data and messages generated on or handled by Board equipment are considered to be the property of the [School District] and not the property of the users of the technology." In addition, the policy mandated that:*
> *[School District] information technology generally must be used only for business activities. Incidental personal use is permissible so long as; i) it does not consume more than a trivial amount of resources, ii) it does not interfere with staff productivity, iii) it does not preempt [sic] any business activity.*
>
> *[18] However, the policy did not provide for the search of the computers nor did it address the issue of privacy, except as it related to e-mail. ..."* (Ontario Court of Appeals, 2011, ONCA 218)

Further, in this school authority, students were required to sign an acceptable use agreement, while teachers were not required to sign, but were informed by the principal that rules applying to students also applied to staff.

Of particular note within the appeal,

> *[45]..." There was no clear and unambiguous policy to monitor, search or police the teachers' use of their laptops."* (Ontario Court of Appeals, 2011, ONCA 218)

The case has been granted leave of appeal to the Supreme Court of Canada, with a decision not expected until 2013.

Policy Considerations

- What steps has your school authority taken to make employees aware of the legal requirements of the legal requirements, legal decisions and ethics that relate to digital environments?
- What steps has your school authority taken to inform students and prepare them for using technologies to in compliance with the law?
- Has your school authority given consideration to what information may or may not sit in the cloud? On local servers? On local computers?

Policy Questions

- Has your school authority addressed bullying and online bullying?
- Has your school authority met requirements under the *Copyright Act* for staff and students? Has it considered the challenge of personal values, ease of copying and the nature of mashups relative to the legal requirement?
- Has your school authority established policy that addresses FOIP requirements?
- Has your school authority been explicit in identifying its right to access data residing on its servers and computers? Who has this right? For what purpose?
- Has your school authority explicitly identified that it will be monitoring network traffic? Has it identified who has this right? For what purpose?
- Has your school authority articulated privacy rights, responsibilities and expectations for employees and students?
- Has your school authority articulated cloud computing opportunities and limitations due to legal requirements?

7. Digital Security

Digital security provides the necessary precautions to best guarantee safety and security. This needs to be addressed in terms of student learning, as well as in terms of protecting students, employees, resources and the organization. While there are numerous technical strategies used to achieve effective digital security, fundamental to this end is a need for leadership to guide technical implementations through policy.

A digital security policy is a critical element in developing a comprehensive security strategy (Alberta Education, 1999a, p.7). More often than not, security is compromised due to people's actions rather than a failure of technologies. Such policy provides an understanding of ownership of responsibility, a vehicle for high-level consideration of security issues and a means of ensuring all members in the organization (students and employees) understand steps to best ensure safety and security.

An important initial step is to understand what and who is being secured. In a school system, one of the primary concerns must be the students within the school authority. Even

in small school authorities, one will often find students under protection - either with legally protected identities or whose identities need to be protected. Access to these students, their personal information or even knowledge of their location poses security risks to them and possibly their family. Protection of their digital information is critical to their protection.

Access to students on the whole is a security consideration somewhat unique to school systems. While some organizations may disregard communications into the organization as an employee or client matter, this is not the case in education. In loco parentis (educator's obligation to act as a natural parent) indicates that school authorities have, and always have had, a security responsibility. Policy is needed to guide personnel and students to enable digital citizenship learning, yet offer security.

Additionally, computing systems and software must be protected. This includes protection of networks, servers, appliances, desktops, laptops, hand-held devices and any other active electronics device. This must occur for several reasons:

- School authorities must ensure protection of data from those who have no rights to the data;
- School authorities must ensure protection of the hardware itself;
- School authorities must ensure protection of software; and
- School authorities must ensure protection of devices from infiltration so it does not become a staging area for other illegal or illicit action.

Finally, school authorities must protect the people within the school authority, as well as the school authority itself. This includes protecting employees' private information, protecting their identity and protecting the storage and transport of their information. Frequently, personnel need guidance as part of policy implementation. Incorporating education to meet the policy objectives is often necessary. Policy can offer both rights and responsibilities. Additionally, the school authority itself needs protection. Its reputation and representation can be at risk. This is accomplished by securing information and by ensuring processes are established to provide direction in how the school authority is represented. Living in the 21st Century with ubiquitous connections world-wide heightens aspects of security considerations.

A starting point for addressing digital security policy is to ascertain the potential risks associated with information technologies and information technology use. These risks may include:

- Personal risk by students or employees (e.g. excessive self-revelation or cyberbullying);
- The risk of inappropriate access (e.g. enabling access through password sharing);
- The risk of inappropriate communications between or with students (e.g. organizations unable to trace communications to students);
- The risk of loss of data from servers (e.g. hackers or inappropriate technology management routines);
- The risk of loss of data by personnel (e.g. stolen laptops, misplaced memory sticks, lost backup media);
- The risk of data loss across the network (e.g. non-secure telecommunications rooms);
- The risk of viruses and virus containment (e.g. infecting one's own systems and partnering organization systems);
- The risk of student transgressions affecting either internal or external digital resources via school authority networks (e.g. identity theft, hacking remote systems or password sharing); and
- The risk of employee transgressions using school authority resources.

Canadian Privacy Commissioner's (2011) office self-assessment tool states:

The reasonableness of security arrangements adopted by an organization must be evaluated in light of a number of factors including:

- *the sensitivity of the personal information,*
- *the foreseeable risks,*
- *the likelihood of damage occurring,*
- *the medium and format of the record containing the personal information,*
- *the potential harm that could be caused by an incident, and*
- *the cost of preventive measures*

Digital security policies should address the high-level security risks identified during the risk management review process. In addressing security risks, policies need to establish a balance between serving the educational and business goals of the school authority relative to minimizing risk – these are not always mutually compatible.

Alberta Education has invested significantly for over a decade in addressing digital security. Some excellent policy suggestions and technical advisories are included in the provincial publications *School Technology Services: Self-Evaluation Guide* (2011), *Computer Network Security* (1999) and the *WLAN Best Practices Guide - Chapter 4 (2007)*. Additionally, to aid with policy implementation, Alberta Education hosts training in information security management for IT leaders and IT staff (2011-2013).

Policy Considerations

- Has your school authority conducted a risk audit to identify risk areas and processes for managing digital risk?

- Have risk policies effectively balanced risk relative to the educational and business goals of the school authority?
- Have your school authority policies addressed various terms of service?

Policy Questions

- What policies does your school authority have in place to protect students and employees in digital contexts?
- What policies does your school authority have in place to protect private and confidential digital information?
- What school authority policies are in place to ensure data integrity and system reliability through backup services, through redundancy and through disaster protection processes?
- What school authority policies are in place to protect system resources (networks, servers, software and intranet resources)?
- What school authority policies are in place to protect the organization itself in digital contexts (e.g. reputation and representation of the organization)?

8. Digital Health and Wellness

Digital health and wellness refers to physical and psycho-social well-being in a technological world. Given the ever-increasing frequency with which students use technologies, particularly in their personal lives, health and wellness are areas that need to be addressed in the interest of developing well-balanced future citizens.

In the physical health domain, the ergonomics of the work station have become more important than ever, given the frequency and duration of use of technologies. Some injuries that can be avoided include repetitive stress injuries, eye strain and carpal tunnel syndrome. Simple solutions such as table height or screen placement can preclude health problems.

In the psycho-social domain, it is recognized that a cultural shift is occurring with respect to what is expected of individuals in social settings, in relationship with others and especially in relationships with others through and with technology. The nature of highly mobile and highly connected technology will continue to place pressure on the nature of social connectedness, both physical and virtual.

There is increasing concern that some people are becoming Internet addicted – namely exhibiting compulsive behaviour that interferes with normal living and causes high levels of stress on family, friends and one's work environment (Young, 2009). Achieving balance will likely become an increasingly relevant characteristic of healthy citizens. Policy can play a role in guiding students and personnel as they seek balance.

Policy Considerations

- What steps has your school authority taken to educate and lead employees and students to lead balanced lives?

Policy Questions

- How does your school authority policy address physical and psychosocial well-being for students to support their increasing use of technologies?
- How does your school authority policy support employee well-being as they increasingly rely upon technologies in their work?

9. Digital Rights and Responsibilities

Citizenship and involvement with any community involves two elements: rights and responsibilities. When membership is provided within a given country or within a given community there are certain rights afforded and with those rights come responsibilities. Digital communities similarly have rights and responsibilities. When a student is given the right to the Internet as part of their education, there are expectations and responsibilities that come with this right. The student affords and expects safety and security when online, respect for shared ideas and fair treatment of resources created and shared via the Internet.

The challenge for education is affording rights and responsibilities on a sliding scale such that students in Kindergarten are not afforded the same responsibilities or rights as students in Grade 12. By Grade 12, students have had at least a dozen years of opportunity to develop citizenship, and now digital citizenship skills and knowledge. Kindergarten students have obviously had mere months and lack the developmental levels for some of the needed responsibilities and subsequent rights.

Defining this sliding scale presents a challenge for policy-makers, but as a starting point, identifying a broad philosophic stance serves all students. Does the organization support students' living *one life* or *two lives* (one life at school and another life outside of school (Ohler, 2010))? Does the philosophic statement recognize the fundamental nature of change occurring in society through technology and the subsequent importance of learning with technology to prepare students for social and work lives?

If the organizational philosophic statements are of this order and subsequently support digital citizenship instruction, then the next step is to ascertain how much control and

management is needed within the organization. How can the organization develop digital citizens? Well-prepared digital citizen students will reduce the need for control and management offered through strictly stated acceptable use policies. Well-prepared digital citizens also reduce the need for technical control.

Policy Considerations

- Has your school authority taken a sliding scale approach to responsibilities and rights for students from Kindergarten to Grade 12?
- Can students expect fair and appropriate treatment in an online context – due in large part to their education and development in digital citizenship?

Policy Questions

- What is your school authority's broad philosophic statement with regard to preparing digital citizens? Does it recognize that broad societal change through information technologies is affecting students' future social and work lives?
- What is the balance of acceptable use policy (control and management) requirements relative to digital citizenship support (offering education and preparation)? Are there procedures and instruction to guide each?)

The Nine Elements: A Thematic Approach

When developing policy, the discrete nature of the above nine elements may prove somewhat unwieldy. To create a more easily comprehendible and yet comprehensive model, it may be helpful to think about these nine elements as framed by Churches' (2011) Respect and Protect model identified earlier. The nine elements may be organized into three overall themes: 1) Respect and protect yourself: Digital well-being; 2) Respect and protect others: Digital interactions; and 3) Respect and protect intellectual property and others property: Digital preparedness. These nine elements fit into the themes as follows.

Respect and Protect Yourself: Digital Well-being

- Digital Security: Electronic precautions for self-protection
- Digital Rights and Responsibilities: Freedoms extended to those in a digital world
- Digital Health and Wellness: Physical and Psychological well-being in a digital world

Respect and Protect Others: Digital Interactions

- Digital Communications: Electronic exchange of information
- Digital Etiquette: Standards of conduct or procedures online
- Digital Access: Full electronic participation in society

Respect and Protect Intellectual Property and other Property: Digital Preparedness

- Digital Law: Responsibility for actions and deeds using electronics

- Digital Literacy: Process of teaching and learning about technology and the use of technology
- Digital Commerce: Online buying and selling of goods

The above nine elements are intended to assist school authority leaders in thinking through the facets of how and where digital citizenship may come to the fore. These elements are also intended to assist stakeholders with a comprehensive approach to digital citizenship policy development.

Within a policy development context, it is important to implement a comprehensive set of policies that include broad guidelines, rather than a series of specific policies for specific situations. Too many policies are not only difficult to implement in schools, they are also equally difficult to regulate. Policies or regulations that are too burdensome will not meet the heterogeneous needs of students or staff. Thus, the above nine elements' descriptions, and the associated policy considerations and policy questions, are not intended as individual policy elements, but rather are intended as considerations and questions to help guide conversations within school authorities. Pending the outcome of conversations with multiple stakeholders during the policy development process, the results somewhat paralleling the above may be found across various policy levels including board policy, administrative regulations, school authority guidelines and school policy.

Current Digital Citizenship Policy Issues

In addition to the nine elements of digital citizenship, two contemporary digital citizenship policy issues - cloud computing and personally owned devices - must also be addressed.

Cloud Computing

Cloud computing refers to the use of remote servers across the Internet to store, manage and process data. A key feature of cloud computing is that it tends to be fairly transparent to the user, yet rather opaque to understand at any level of detail. For example, while using a cloud computing service is easy for the user, the physical location of the end server(s) is not known. It is typically possible to trace the location, but the invisible and transparent nature lends to a *cloud experience*. A cloud service can be public, wherein the service is sold to anyone, or it can be private wherein the service is sold to a limited number of people.

While cloud computing may be as simple as data storage and retrieval (e.g. DropBox), it may also provide a deeper experience for the user. For example with Facebook or Wikispaces, not only is data stored on a remote server, it also provides a service deeper than simple file storage – it connects people.

Cloud computing and the nature of interactions through such transparent tools is a key element driving the current necessity for digital citizenship policy. As youth reach out beyond their immediate environment through pervasive connectedness enabled through cloud computing, they and their parents ask, "What is the school's role and responsibility in preparing students for living and working in a digital world?"

Branigan-Pipe (2011) echoes this concern in her reflection:

> *As a parent, I worry that my children, while in school, are not experiencing the realities that technologies offer in the real world. As a parent, I worry that my children are being limited at school and are not accessing their full potential due to both the lack of infrastructure in schools, as well as the lack of teacher education around the use of social media tools as educational resources and literacies.*
>
> *As a teacher, my worry for my students is mostly about online safety (although I also worry that we are missing a big opportunity to prioritize a medium that has become dominant for most of our children). I know that my students are using social media the moment school ends (Facebook, Twitter, texting, MMORPG's….). But who is teaching these skills?*

Branigan-Pipe identifies a key concern for educators, for administrators and for policy-makers: "How do we keep our students safe as they learn to become digital citizens?"

While there are no simple answers to this question, Levinson and Socia (2010) offer a few recommendations for educators to address some of the issues surrounding cloud computing:

> *First, review appropriate use agreements with the students, anticipate potential problems that might arise and arm the students with strategies to overcome potential obstacles or concerns. Have students create the norms for use and develop consequences if there is a violation of the norms.*
> *Second, communicate the goals of using the new tool to parents. Hold a parent meeting to introduce the application. Have students and parents come together to use the application, with students showing parents how to use the application.*
> *Third, provide ongoing communication and support for students and families. These three simple steps would go a long way toward helping students and parents maintain a positive outlook toward technology in schools and create community around collaboration opportunities for students and parents.*

There are additional recommendations that also will support educators as they strive to create safe learning environments in a cloud computing context. The following sections will share some of these recommendations.

Know the Terms of Agreement

A good starting point for keeping children safe is understanding the nature of the agreement that individuals and school authorities make with cloud computing services. Specific cloud computing services typically require an agreement through the terms of service. These may differ significantly across various cloud computing service providers. For example Facebook, as a social media site with over 750 million participants, encourages storage and sharing of personal data and works to protect individual privacy (see Facebook Terms of Service). WikiSpaces, on the other hand, serves over 5 million people and specifically states within its terms of services that users agree not to store personal data about other users.

Terms of service agreements tend to differentiate youth based on the age of 13 years. Under federal law in the United States, the *Children's Online Privacy Protection Act* of 1998 (COPPA) identifies age 13 as a demarcation for online participation that involves collecting personal information. Hence, various terms of service address COPPA in various ways. Facebook's terms of service do not permit children under 13 years of age to use its site. Wikispaces' terms of service allow children under 13 to use their service with parental consent; teachers may create accounts for students, but Wikispaces then presumes teachers have parental consent. A Facebook alternative for children, Togetherville, encourages youth under age 13 to participate, but accounts are established only through verifiable parental consent.

While Facebook, Wikispaces, Wikipedia, blogs (e.g. Edublogs, Blogster), Google Docs, Twitter and YouTube receive significant public attention as examples of cloud computing, there are many, many cloud computing services that offer tremendous learning value to students.

A distinction among types of cloud computing services may be helpful. Some cloud computing services are highly social in nature. For example, Facebook and MySpace began largely as social media environments – and a significant focus remains on the social element. Other cloud computing services, defined here as Web 2.0 services, have a more direct educational application. They enable geographically independent collaboration and problem-solving with an increased learning focus. GoogleDocs, Bubbl.us and Wikispaces all fall into this type of cloud computing service. Still, other cloud computing services

primarily focus upon offering an educational application with limited collaborative opportunity. These would include Timetoast, Wordle and BrainPop.

Policies may need to accommodate these subtle differences between social media and Web 2.0 applications. For example, socially-oriented cloud-computing resources may be viewed differently than those resources identified as educationally oriented.

Teacher Preparedness

Teacher preparedness is a second and highly important vehicle for better ensuring student safety – and teacher safety. The cloud computing examples provided above are but a sampling of the many cloud computing services available to students and educators. Some degree of risk resides in all of these services - with some services holding more risk than others. However, risk need not be a deterrent.

If students are to be prepared for living and working in a digital context, where digital citizenship serves as a foundation for tomorrow's citizens, then educators need to have an opportunity to work within a set of policies that guide their development and professional work. A digital citizenship policy is needed for the school authority to create both momentum and resourcing to best ensure that student safety is paramount as instruction incorporates cloud computing. Professional learning opportunities are needed to support and encourage educators in the use of Web 2.0 and cloud computing tools. Well-articulated parameters are needed to guide teachers as they work within the bounds of school authority direction.

Account Management

While individual staff members may be responsible for setting up their cloud computing service as part of their teaching and while students may be responsible for working through their teacher to establish cloud computing services, there remains a need to understand who has rights to access each of these accounts.

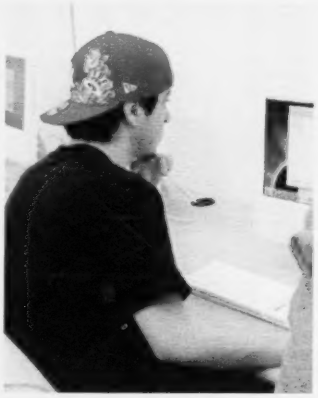
When services were managed through an organization's intranet service, for example e-mail offered through the school authority, it maintained some degree of control over the given account(s). If a teacher left employment with the school authority, the account was removed. If an employee ill-represented the school authority using such services, action could be taken in conjunction with the employee and the account. If a student used school authority services in inappropriate ways, it could manage the account to address behaviour.

In the transition from intranet accounts to cloud computing accounts, conversations with stakeholders as part of the policy development process will serve organizations well. If the school authority opts to exercise rights to cloud computing accounts, it is imperative that employees and students are aware of such management controls. Parameters would be

necessary to guide employees and students, as well as administration, to know what behaviour is acceptable. As well, the policy would need steps taken in the event that some choose to work outside the parameters. Alternatively, one must ask, "Are there new paradigms of responsibility and management, given the new paradigm of service?" Does one or must one engage in the same level of acceptable use management as conducted historically?

Freedom of Information and Protection of Privacy Act

The *Freedom of Information and Protection of Privacy Act* (FOIP) requires that personal information be protected. When using cloud computing services, one cannot share personal information about others unless the prescribed procedures within FOIP are followed. The term *personal information* is key and fully defined within the legal act (Appendix C).



As shared in the earlier section on Digital Law, FOIP legislation also presents limitations on storage of personal information on servers residing in foreign locations. Contravening the FOIP Act can result in substantial fines for individuals or school authorities.

Cloud Computing Synopsis

There are significant educational opportunities and challenges as educators and educational organizations reach beyond their traditional boundaries. The obvious and easy answer to avoid the challenges associated with cloud computing is to simply preclude or severely limit its use. Ohler (2011) points out the difficulty with this approach by asking – "Two lives or one?" Students are asked to live *two lives* when they are required to unplug from global connectivity as they enter school and then return to another life with a digital reality encompassed by much of society outside of school. If students are asked to independently learn issues of digital citizenship, cyber safety and responsible use on their own – it is often done through peers.

If school authorities opt for the *one life* model, they assume the important role of helping students understand issues of digital responsibility, cyber safety and becoming citizens who understand living and working in a digital context. They help students to balance individual empowerment through digital technologies with a sense of personal, local and global responsibility. Critically, schools blend student lives where they integrate and apply fundamental learning from school-to-home and home-to-school. Educators recognize the power of collaboration, of group-task problem-solving and of intercultural and global learning. Policy provides an understanding of the level of responsibility assumed by stakeholders in preparing students for *one life*.

Policy Considerations

- What are the specific terms of agreement or the statement of rights and responsibilities for each cloud computing agreement? Does your school authority hold any responsibility for such agreements when conducted as part of instruction or administration? Who is responsible for overseeing instructional and administrative terms?
- How will your school authority manage training and preparation of staff to ensure their knowledge and skills-base are sufficient to meet the policy requirements?
- Are your staff and students familiar with digital citizenship guidelines as they use cloud computing resources? How has your school authority assisted staff and students in gaining familiarity?

Policy Questions

- Who owns the cloud based accounts when prepared as part of employee duties or student learning? What rights does your school authority have to access employee and student cloud-based accounts when these accounts are used in the performance of their duties? Are there legal implications?
- Will your school authority reserve the right to access employee and student cloud computing services? How will the logistics of such access be managed? (e.g. Will school administrators oversee teacher accounts and teachers oversee student accounts?)
- Will any training be required in advance of opening cloud computing accounts? Will instruction in digital citizenship be part of the expectations or requirements?
- Will students be permitted to open cloud computing accounts? Will parents be invited for parallel training? Will parents be informed or will consent be required for their child's use of cloud computing services? What is the age range for such consent?
- Are all employees aware of the FOIP requirements when using cloud-based accounts? Are they aware of the nature of information that may be placed in a cloud-based account and the nature of personal information that may not?
- Are there policies (e.g. guidelines) in place that require specific digital citizenship instruction prior to student use of given cloud-based activities?
- How will your school authority handle violations to cloud computing policy?

Bring Your Own Devices and Digital Citizenship Policy

Increasingly students arrive at the doorsteps of schools with their own personalized technologies in hand. Personally owned devices and Bring Your Own Device (BYOD) models are being adopted within schools and school authorities, which provide meaningful learning opportunities for students. Students are already familiar with the operations of their

own device. These devices can be tailored to the specific learning needs of the individual student – whether this involves simply changing font sizes or changing the interface to a Braille input to accommodate student learning needs.

Students are also able to access the same device 24 hours a day, seven days a week, which bridges formalized learning with informal learning settings. Learning is no longer delineated as predominately occurring only within the bounds of school, but rather a multi-environment and, ultimately, a life-long experience. A single platform for learning increases student connectivity, creativity and confidence.

Additionally, there are pedagogical benefits that may be realized through personally owned devices. Personalized learning is enabled through high-levels of access to tools that are highly familiar. Participation in collaborative learning is effected through BYODs and Web 2.0 technologies. Finally, BYODs offer full participation for students who may demonstrate learning challenges without ongoing access to their device.

Alberta Education has developed a guide for school authorities allowing students and staff to use their own devices on school networks. *Bring Your Own Device: A Guide for Schools* addresses how school authorities can implement BYOD models and discusses the considerations needed for BYOD models in greater detail. This includes digital citizenship considerations, technical advice and a framework for school authority readiness. Challenges related to digital citizenship and BYODs are considered in the BYOD guide.

Some nuances are presented when introducing BYODs. For example, consider traditional approaches to managing illicit material. At one time, when students brought illicit materials to school, the school could confiscate the photo or text. Given the virtual nature of illicit material today, it is the vehicle, the device that transported the illicit photo or text that is typically at question rather than the digital photo itself. What are the school authority's rights and responsibilities in confiscating a student-owned learning resource that has transported illicit material? What rights have educators to preview a student-owned device when suspicions arise? How can a school authority best protect students when communications occur on a private, personalized device – especially if such communication occurs via a 3G or 4G non-school authority-owned network? Policies have a role to play in answering these questions.

In the future, the demand for use of these devices will likely prevail as educational applications are adopted, as prices of devices continue to fall and also as students begin arriving with their own network plans that potentially ignore school provided network services. This has several implications including an increased need for digital citizenship

instruction; the need to ensure all students have equitable high levels of access to online information and communications; and an inability to block information flowing to and from students via the school authority network using traditional content management systems.

While the occasional solution has been to ban student-owned devices, this approach fails to address student learning needs. With such a ban, the tremendous learning opportunities afforded through BYODs are lost. Personalized learning through high levels of access is lost. The bridging of formalized and informalized learning is lost. Yet, the tremendous educational opportunity and the associated challenges arrive as one package. Digital citizenship policies and digital citizenship instruction are part of the solution.

Policy Considerations

- Has your school authority strategically and actively prepared students as digital citizens to best prepare for engaging students using BYODs?
- Does your school authority network currently have sufficient wireless capacity, network capacity, supports and management to handle BYODs?

Policy Questions

- Have the nine elements of digital citizenship been effectively addressed in preparation for BYODs?
- Have educators received ample supports to realize effective pedagogical benefits associated with personalized learning through BYODs?

5. Digital Citizenship Process and A Road Map

Leadership

Given the pervasive nature of information technologies across all aspects of educational organizations, digital citizenship policy development requires senior level leadership. Attempts to parse out digital elements, by delegating such responsibilities to information technology teams, will not support the long-term direction of learning, leadership and administration. The breadth of roles and responsibilities that digital citizenship policies will affect within school authorities suggests the need for senior level decision-making. Senior level leadership serves a critical role in leading the development of a digital citizenship policy and in overseeing stakeholder involvement.

Stakeholder Involvement

Under the direction of senior leadership, stakeholder involvement is fundamental to effective policy development and direction setting. Stakeholder involvement is critical during policy development (Lencioni, 2002) and more so during the development of policy that deeply encompasses values and ethics, such as frequently encountered within digital citizenship policy development.

Stakeholder involvement will resolve two important factors in policy development. First, the consultative approach will develop a stronger policy through balancing varied perspectives brought forth by a broadly representative team. Second, it will move toward a strategy for effective policy implementation gained through involvement of stakeholders and a mirroring of stakeholder interest.

The process associated with developing a digital citizenship policy is an extremely important element. The process is at least as important as the ultimate product (i.e. the digital citizenship policy). Conversations which help move the organization to common understandings about the nature of the values and the associated culture within the organization are critical. While a top-down approach of pre-determining the policy document may expedite the process, it will leave little room for involvement of stakeholder views that ultimately contribute to the implementation and values behind the policy.

If meaningful stakeholder involvement serves a fundamental role, then the next question is, "Who are the stakeholders to include in these conversations?" The stakeholders are those people for whom the policies are salient and who ultimately will help the policies realize effective implementation.

The stakeholders one might involve in digital citizenship policy development should represent those members of the community for whom the digital citizenship policies have relevance. In addition to senior leaders, this might include:

- School Administrators
- Teachers
- Students
- Community Partners
- Information Technology Staff
- Parents
- Support Staff
- Communications Staff

The process of stakeholder involvement may take several different forms. Central to involvement, though, is engagement in the process, opportunity for voicing ideas and respect for different perspectives. While not all stakeholders can be involved in all phases of the process, broad representation presents strengths.

A grassroots process may involve all stakeholders participating in a survey at the start to gather stakeholder thinking. This survey is then used by a decision-making committee to formulate draft policy. The draft policy may then be refined through a vetting process involving various parties.

Alternatively, a more directed process may ask the policy team of core stakeholders to prepare a preliminary draft of a policy. The preliminary draft would then be vetted to a broader audience for further conversation, insight and refinement. Vetting may include key players not represented or insufficiently represented within the decision-making committee. Vetting may occur across individuals, for example all teachers or all secondary students, or it may be vetted to organizations, for example the local ATA executive or secondary school student unions. A formalized process is needed for garnering information from these groups and for incorporating these thoughts back into the policies under consideration.

Digital Citizenship Policy: Three Layers

It is suggested that digital citizenship policy development occur as a layered approach. For example, at the outer layer is a broad school authority-based policy, possibly a board policy, which provides philosophic direction in terms of digital citizenship beliefs, makes connection to associated broader requirements (e.g. provincial legislation) and may offer a broad framework for employees, educators, students and parents. Offering more detail is the next layer, the administrative regulations. These regulations provide clarification of key

concepts offered in the policy and may indicate the necessary actions and who shall assume responsibility. Finally, given that digital citizenship policy is a relatively new domain in school authorities, there is a need to provide procedures or guidelines. The procedures provide greater levels of specificity to assist in the implementation of regulations. These help staff enact the policies by providing specific directions that may be carried out at the field level.

An example in brief may be helpful. The intent of this example is to provide a flavour of the various layers from board policy to administrative regulation to guideline. The specific names of these policy levels and the format of these policies will differ across school authorities. It is not intended to suggest that any of the following examples are complete or fully represent the reader's context or needs. Rather the intent is to provide the flavor and sense of direction attained through three layers: board or administrative policy, administrative regulation and school authority procedures.

Layer 1: Board or Administrative Policy

The first of three layers is the administrative or board policy. It shares a philosophic statement providing overall guidance and authority for the organization to work within the philosophic direction.

> **Example Administrative or Board Policy:**
> The Anytown School authority No. 1234 recognizes the important role contemporary media and digital connectedness plays in educating students and preparing them for lives that encompass working, socializing and learning in digitally enmeshed environments. In light of these social and educational changes, the school authority encourages the use of information technologies to prepare students as digital citizens and life-long learners.

Layer 2: Administrative Regulation

The second layer is the administrative regulation. The regulation follows from administrative or board policy. It is in keeping with and builds upon the administrative or board policy. This layer provides detail and also has policy authority to guide and take action on behalf of the organization. In this particular example, it is founded in provincial legislation, the *Freedom of Information and Protection of Privacy Act* (FOIP).

> **Example Administrative Regulation:**
> *Administrative Regulation #567: Privacy and Protection of Personal Information **
>
> ** Note: The conceptual base for this Regulation and the following Guideline are drawn from Wolf Creek Public Schools, Administrative Procedure #169. Used with permission.*

Background
Anytown School Authority No. 1234 manages student, parent and employee information as part of its mandate. The Alberta *Freedom of Information and Protection of Privacy Act* makes provisions for ensuring that information privacy is maintained on all personal information.

Records containing personal information may be stored in paper or electronic forms. Care must be taken to ensure privacy of all such information when in the custody of the school authority. Specific care must be taken when such information is stored on electronic media or on portable information devices.

Definitions
Electronic media will include DVDs, CDs, USB flash drives, backup tapes and other media forms that store text or media in electronic form.

Portable information devices will include all forms of digital devices that hold information in electronic form. This will include such devices as tablets, laptops, Blackberries, iPods, iPhones, smartphones and other electronic devices that are mobile in nature.

Personal information is defined within FOIP as (the full definition as shown in Appendix C).

Confidential information is defined as any information that is personal in nature but not included in the FOIP definition. This would include student Individual Program Plans, information on protected students, student grades and records private to students, their parents and teachers.

Requirements
All principals and managers will ensure that their staff is aware of responsibilities as detailed in Anytown School Authority Procedure #8910. (This would be the associated procedure which supports implementation of this administrative regulation.)

All personal and confidential information stored on portable information devices must be encrypted and password protected using passwords that meet Anytown School Authority Guideline #1112. (This referent guideline is not provided herein.)

Employees will ensure that portable information devices are protected from theft by keeping such devices in secure areas.

Employees shall immediately report all incidents involving personal information to their supervisor. This includes theft, loss or unauthorized access of portable information devices.

Violating this administrative regulation may result in disciplinary action pending the severity and nature of the incident and actions.

Layer 3: School Authority Procedures or Guidelines

The third layer is the procedure layer. The procedure supports school authority policies by providing guidance and instruction to help enable members of the school authority to meet the policy requirements. While the policies answer *what* and *why*, the procedures answer *how* or *when*. Procedures have the flexibility of change without significant administrative overhead. This can prove of value in a domain where the specifics may change with some frequency.

Anytown School Authority Procedure #8910

These procedures support the privacy protection of personal information and best ensure confidentiality of information as per the FOIP Act and Anytown Administrative Regulation #567: Privacy and Protection of Personal Information.

Portable Information Device Security

The first level of protecting student information is to best ensure that portable information devices are secure. Physical security of these devices serves as a first level of security.

1. Members of Anytown School Authority will keep portable information devices in a secure location (e.g. locked car trunk, secured handbags).

2. Ensure portable information devices are labeled with contact information in case of loss.

3. Immediately report theft of a portable information device to the local police and inform the police of the nature of information loss.

4. Immediately report in writing to your supervisor the theft, loss or unauthorized access of portable information device. Provide a copy the report to the Superintendent of Schools.

5. Document an inventory of personal information and confidential information that was stored on the lost portable information device. Access to a backup of the device may be helpful for this purpose.

6. In the event of a breach of personal information, the principal or division administrator will send a notification letter to all whose information has been compromised, advising of the potential inadvertent disclosure of information. Depending upon the nature of information compromised, it may be necessary to inform immediately.

The second level of protecting information is to provide technical security supports through management features and encryption.

7. All portable information devices will use a minimum of 128 bit encryption to protect data. Encryption will limit access to the data without the necessary password.

8. All portable information devices must offer remote wipe features to enable the removal of data from the device in the event of loss or theft.

9. Consult members of the Information Technology team for support, to receive technical guidance and to ensure effective encryption strategies.

The third and critical level of protecting information is the creation of effective passwords. Passwords will follow the password strategy as defined in Guideline #1112 (Guideline #1112 example not included). In brief review, passwords as described in the guideline:

- Must be treated as confidential information;
- Must be stored in encrypted form;
- Must be a minimum of eight characters and digits in length;
- Must include both characters and digits;
- Must not be dictionary words; and
- Must not contain personal information.

Anytown Procedure #8910 has been formally approved for implementation, effective March 1, 2012.

Through the overall process of policy development, stakeholders should give consideration to core digital citizenship elements by examining the nine digital elements, as well as those elements considered under current digital policy issues. Leaders may wish to prioritize the list of policies that need to be addressed and identify those that are needed in the immediate term versus moderate-term or long-term.

Policy Outcomes

Using the above strategies for digital citizenship policy development, various school authority communities will meet outcomes in a manner that represents their specific school authority culture and context. Stakeholder involvement serves to tailor outcomes to this end.

As one explores implementing meaningful policies, one may consider three types of legal approaches summed up by Solove (2009):

> *"What can and should the law do? From the bird's-eye view, there are three basic approaches the law might take. First, the law could take a libertarian approach and remain as "hands off" as possible. Second, the law could adopt an authoritarian approach and attempt to radically limit the ability of people to spread information on the Internet. Or, third, the law could take some middle-ground approach between these extremes."*

Some may argue that relative to digital citizenship policies, acceptable use policies have largely assumed the second position, an authoritarian approach. For a period of time, this approach was successful and met organizational needs. However, in today's context, this position of limiting access to digital technologies in educational contexts fails to serve students, given that in their *other life*, beyond the boundaries of school, they continue to reside in pervasively connected, highly mobile digital environments.

However, swinging the pendulum to the first position is equally threatening for students. A fully open libertarian approach equally presents risk to students. While guidance of students through digital citizenship is sorely needed and will help many students effectively navigate this new information and communications vehicle safely, instruction per se may not be enough.

The third position, a middle-ground, may prove the most successful outcome. School authority approaches will likely most closely resemble some variant of this third approach. Digital citizenship policies provide guidance and instruction, yet parameters are also in place to identify the boundaries of participation.

Road Map to Digital Citizenship Policy Development

Where to start? This may be the next logical question. The current work has offered a comprehensive view of digital citizenship policies. The challenge is to take this comprehensive understanding and implement policies that are meaningful within the school authority's culture and context.

The Road Map to Digital Citizenship Policy Development (Figure 2) is intended to guide readers in the steps toward effective policies. The starting point within the road map is a Digital Citizenship Needs Assessment Tool (Appendix D). The needs assessment tool will guide school authorities in determining both whether such policy requires attention and which particular elements require attention.

To develop digital citizenship policy, senior leaders are encouraged to involve stakeholder decision-making. Note that not all stakeholders will be versed in societal and local contextual considerations, provincial and federal legislation and educational, as well as administrative, aspects of the school authority. This guide will assist in providing some of this background. The "Resources" (Chapter 7) section of this Guide can assist the reader and members of stakeholder groups in gaining background.

The Digital Citizenship Needs Assessment Tool will assist school authorities in identifying priorities. Members of the stakeholder group will then reference the nine elements and the two current digital policy issues to hone policy that meets the contextual and cultural needs of the local school authority.

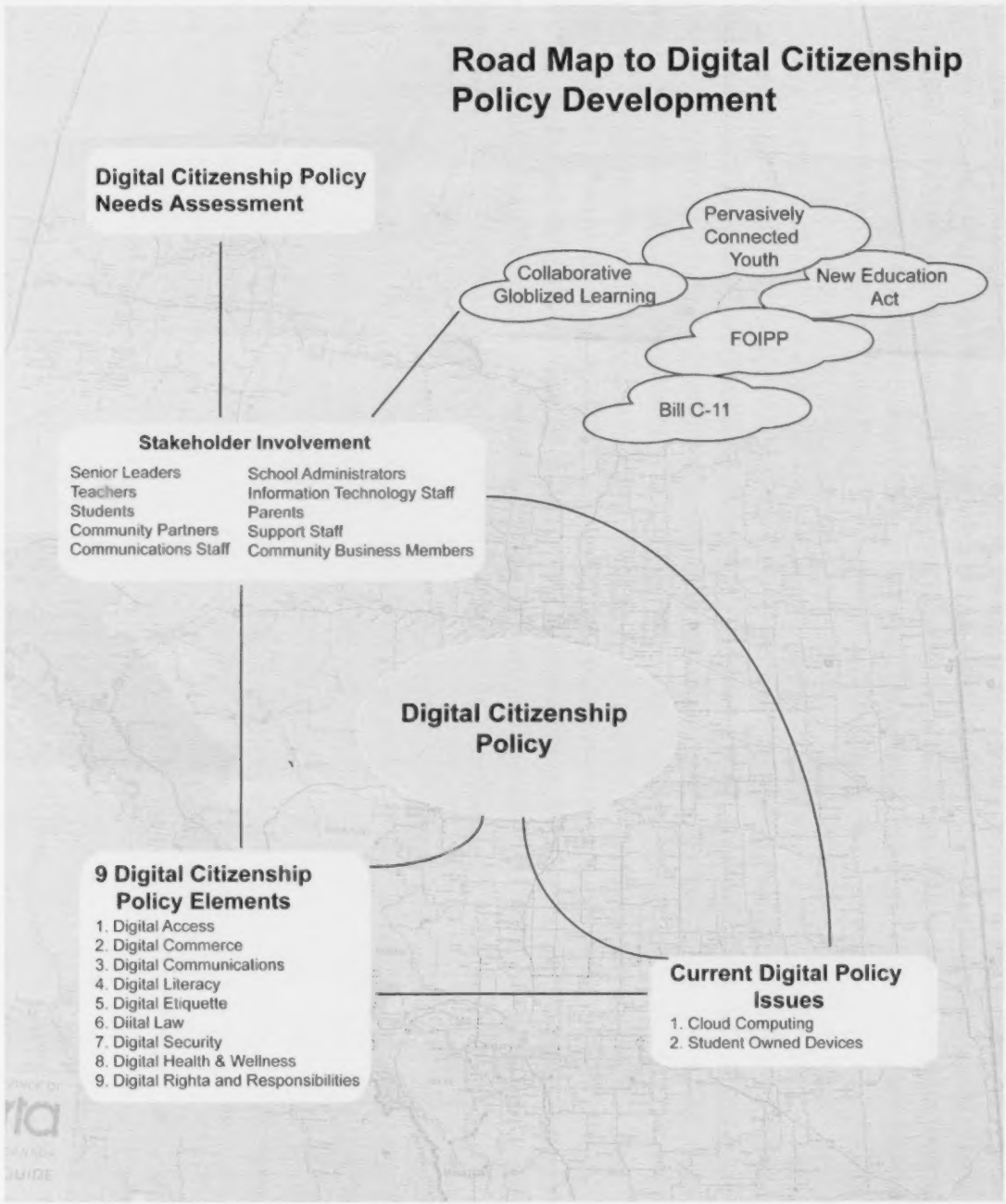


Figure 2: Road Map to Digital Citizenship Policy Development

6. Conclusion

This work is based upon an extensive literature review and numerous formal and informal conversations with senior leaders across Alberta.

Acceptable use policies have historically filled an important role for school authorities for many years by providing parameters and a sense of direction for personnel and students. Changes in technologies, society and the workplace have in-turn effected expectations of the education system and subsequently the nature of attendant policies. Leaders have sought guidance as they reexamined their acceptable use policies.

Work within the field of digital citizenship provides a strong base for developing policies that are thorough and comprehensive. Ribble's (2011) work provides a framework of nine elements that help guide digital citizenship policy considerations and questions. Additionally two current digital citizenship policy issues, cloud computing and BYODs, assist leaders with contemporary challenges. Leaders and stakeholders can use these 11 elements and the associated policy considerations and questions as a means for thinking through the various avenues of digital citizenship policy.

The process for developing digital citizenship policies is one of involving stakeholders that represent the culture and community of the school authority. Building upon conversations and direction from stakeholders, leaders are able to build a layered approach to digital citizenship policies. These layers encompass broad philosophic direction, down to procedures that will assist personnel and students in fulfilling regulations within the organization.

Comprehensive digital citizenship policy development will lead school authorities to meet provincial and federal legislative requirements; best position authorities for contemporary student learning; ensure student safety while enabling high levels of access to communications and information; care for student and employee security and well-being; and provide guidelines to support school authority, student and employee connections to the world.

Through effective digital citizenship policies, school authorities are able to balance safety and security with contemporary meaningful instruction which, as Ohler (2010) suggests, enables students to lead *one life* - a life that assumes schools have a significant role to play in guiding and enabling students through the power of collaboration, group-task problem-solving and intercultural and global learning.

7. Resources

All the resources provided are intended to provide school authorities with additional information on digital citizenship and digital citizenship policy development. The information provided in these articles, reports or websites does not necessarily reflect the opinion of Alberta Education.

Background Resources

Moving Beyond One Size Fits All With Digital Citizenship – This article provides excellent background on the nature of digital citizenship needs and the stages (e.g. solutions and non-solutions) sought through education. Link to the article: http://publius.cc/moving_beyond_one_size_fits_all_digital_citizenship

Character Education for the Digital Age (Ohler, 2011) – This Association for Supervision and Curriculum Development (ASCD) article provides a synopsis of the needs for addressing digital citizenship and describes the ideal school board. Link to the article: http://www.ascd.org/publications/educational-leadership/feb11/vol68/num05/Character-Education-for-the-Digital-Age.aspx

Meeting of Minds: Cross-Generational Dialogue on the Ethics of Digital Life. This publication will assist in thinking about dialogue and the differences in perspective between generations. Several key considerations are made with regard to social media and Web 2.0 contexts. Link to the document: http://www.macfound.org/atf/cf/%7Bb0386ce3-8b29-4162-8098-e466fb856794%7D/DML-FOCUS-DIALOGUE-REPORT-0910.PDF

Bring Your Own Devices: A Guide for Schools
A province-wide community of practice developed this guide that examines the use of Bring Your Own Device (BYOD) models in schools. It looks at the potential opportunities and benefits, as well as the considerations, risks and implications that arise when schools allow students and staff to use personally owned devices. Link to the guide: http://www.education.alberta.ca/media/6724519/byod%20guide%20final.pdf

Policy Resources

Policy Development Processes. The process of developing policy in the digital citizenship arena has some parallels with the processes identified in Supporting Safe, Secure and

Caring Schools (Pages 29-45). Link to the online document:
http://eric.ed.gov/PDFS/ED467674.pdf

St. Marys City Schools Bring Your Own Technology Policy – A policy that guides students and parents in the rights, responsibilities and limitations associated with using their own personal device while on campus. Link to the online document:
http://www.smriders.net/assets/pdf/BYOT-AUPv2.pdf

Wolf Creek Public Schools Protection of Personal Information and Privacy (Procedure #169) – A policy that addresses privacy of personal information and also addresses personal information devices in that context. Link to the online document:
http://www.wolfcreek.ab.ca/Procedures100?object=/documents_directory/Procedures%20(admin)/Section%20100%20General%20Administration&inforbar=no%templates=rwd&confposition=2

Wolf Creek Public Schools Use of Technology (Procedure #140) – A policy that addresses appropriate etiquette and use of electronic resources. Link to the online document:
http://www.wolfcreek.ab.ca/Procedures100?object=/documents_directory/Procedures%20(admin)/Section%20100%20General%20Administration&inforbar=no%templates=rwd&confposition=2

Edmonton Catholic Schools Password Protection Policy (Administrative Regulation 129.2) – A thorough description of password requirements across roles and grade levels. Link to the online document:
http://www.ecsd.net/policies_forms/general_school_admin.html

Social Media Guidelines for Schools. A wiki offering direction that may serve as a basis for thinking about policy development or as a basis for building guidelines to serve developed policies. These include guidelines for staff, students and parents. Link to the wiki:
http://socialmediaguidelines.pbworks.com/w/page/17050879/FrontPage

Policy with a Digital Citizenship Direction. At a school authority level, this policy alone is not sufficiently comprehensive, however, it does offer a contrast to traditional acceptable use policies that focus on control and management approaches versus educational approaches. Link to the sample school policy:
http://www.utechtips.com/2009/07/31/aup-driven-by-vision-not-protection/

Millen Woods Public School Personal Devices Responsible Use Policy. A school-based policy for personal device use. It may lack the comprehensiveness needed at a school authority level. Link to the policy:
http://franklinipads.weebly.com/wireless-policy.html

Digital Citizenship Resources

Digital Community, Digital Citizen - Jason Ohler's (2010) book examines digital citizenship and how it fits within the broader context of citizenship of the past and citizenship of the future. Link to the book:
http://www.jasonohler.com/publications/books.cfm

Digital Citizenship in Schools, 2nd Edition – Mike Ribble's 2011 book examines digital citizenship, provides a framework of nine elements and offers lessons associated with the nine elements. Link to the book: http://www.iste.org/store/product.aspx?ID=2111

Digital Citizenship.Net - Mike Ribble's website serves as a core resource in the area of digital citizenship in the classroom. Link to the site: http://www.digitalcitizenship.net/

Educational Origami – Andrew Churches' wiki provides some excellent resources on digital citizenship and 21st Century pedagogy, teachers, learning spaces and assessment. Link to the site:
http://edorigami.wikispaces.com/The+Digital+Citizen

Digizen.org – This website provides information on digital citizenship for educators, parents and youth. It encourages responsible digital citizenship and shares specific advice and resources on social networking and cyberbullying. Link to the website:
http://www.digizen.org/

Digital Citizenship Resources – This website provides content from other sites in a "binder" format. The content is directed at teachers, parents and students with content for students broken into grade ranges. Link to the website:
http://www.livebinders.com/play/play_or_edit?id=34991

Professional Advisory: Use of Electronic Communication and Social Media. This advisory assists educators in differentiating private versus professional use of social media, shares some professional vulnerabilities and describes criminal and civil law implications. Link to the advisory:
http://www.oct.ca/publications/PDF/Prof_Adv_Soc_Media_EN.pdf

Online Safety and Empowerment Resources

UNICEF's Digital Citizenship and Safety – This video speaks to empowerment through online communities. Link to the video:
http://www.youtube.com/watch?v=NOIOFRhDnxg

HCS Digital Citizenship. A hard-hitting promotional video showing the occurrence of sexting and how privacy loss occurs. Link to the video:
http://www.youtube.com/watch?v=N4uc1iVxLxU

Family Online Safety Institute: Building a Culture of Responsibility – A video describing the layers of responsibility and strategy necessary to realize youth safety while online. Link to the video:
http://www.youtube.com/watch?v=__6reHITDWA

Family Online Safety Institute: What's on Your Mind?: The Challenges and Opportunities of Social Networking – A panel conversation from the Family Online Safety Institute's 2010 Annual Conference. Length 1 hour 3 minutes. Link to the video:
http://www.youtube.com/watch?v=uG6CPXnKZaI&feature=relmfu

EU Kids Online (2011). Although not focused on school systems per se, this cross-national research, including over 25,000 student participants, is an excellent resource as one thinks about Internet use, risks and student safety. Link to the report:
http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx (see Final Report)

Security Resources

School Technology Services: Self-Evaluation Guide – Chapter Four of this Alberta Education guide provides extensive guidance in managing security within a school authority. The guide also discusses governance – a helpful element in thinking about policy. Link to the guide:
http://education.alberta.ca/media/6555222/school technology services - self evaluation guide-final.pdf

Computer Network Security Best Practices for Alberta School Jurisdictions – This document provides specific guidance for school authorities in securing computer networks. The opening chapter addresses policy concerns and presents a refined analysis of many policy considerations relative to network security. Link to the guide:
http://www.albertaitmanagementservices.ca/docs/computernetworksecurity.pdf

Information Security Management for IT Leaders and IT Staff (2011-13) - To aid with policy implementation Alberta Education is hosting a training series for IT Leaders and IT

staff across the 2011 to 2013. Link to details and a schedule:
http://education.alberta.ca/media/6619533/isaca_course-calendar_2011-13.pdf

Securing Personal Information: A Self-Assessment Tool for Organizations - Developed by the Canadian Privacy Commissioner's Office, this in-depth tool may be used in full (251 questions) or by focusing only upon those areas most relevant (e.g. risk management, wireless, records management, compliance). Link to the self-assessment: http://www.priv.gc.ca./resource/tool-outil/security-securite/english/AssessRisks.asp?x=1

Instructional Resources

Passport to the Internet for Grades 4 to 8 – Alberta Education has licensed this interactive MediaSmarts resource for Alberta Grades 4 to 8 students. The online resource provides instruction on Internet skills including online safety, privacy management and ethics. Link to the website: http://mnet.hypernet.ca/e/
(Alberta students and teachers can access the resource through www.LearnAlberta.ca.)

MyWorld for Secondary Students – Alberta Education has licensed this interactive MediaSmarts resource for Alberta Grades 9 to 12 students. This online resource is designed to guide secondary students in Internet skills by simulating online experiences youth may encounter. The resource guides students in researching and authenticating online information, managing privacy and reputation, dealing with online relationships and using digital media in an ethical manner. Link to the website:
http://mnet.hypernet.ca/e/
(Alberta students and teachers can access the resource through www.LearnAlberta.ca.)

My Privacy, My Choice, My Life – Guidance from the Office of the Privacy Commissioner of Canada for students, teachers and parents in managing privacy. Link to the website: http://www.youthprivacy.ca/en/index.html

That's Not Cool - Conversations and resources to guide students in managing privacy in a digital world. Also offered are resources for teachers and parents of middle school and high school students. Link to the website: http://www.thatsnotcool.com/

Privacy Tip Sheet – A tip sheet to help parents (and teachers) with issues of privacy. Link to the tip sheet: http://www.youthprivacy.ca/en/tipsheet.html

Protecting your Online Reputation – The video "What can YOU do to protect your online rep?" provides excellent guidance for students in managing online reputation. Link to the video: http://www.youthprivacy.ca/en/video_index.htm

Appendices

Appendix A: Context

Policy Context: A Broad Societal Perspective

Tremendous change has occurred around the world as methods of gathering information, communicating, publishing content, expressing creativity, problem solving and sharing have evolved at a dramatic pace. The rapidity of this change in society as a whole has often found the field of education and educators struggling to stay abreast of such change and effectively meet learners' needs.

Such change is not simply reflective of the past; it is also reflective of the future. It is anticipated that the rate of change will not just continue, but actually increase. Friedman (2005), in his bestselling book *The World is Flat: A Brief History of the Twenty-First Century*, points out 10 forces that bring significant change through a "flattening of our world." This refers to a leveling of the global competitive playing field. In turn, such flattening affects societies in broader terms. These flatteners include the change in political landscape through the fall of the Berlin Wall (at least partly attributable to technological changes), the advent of Netscape which moved information into the hands of the masses in a non-proprietary format, the move to open sourcing which demonstrates that collaborative communities could develop resources (e.g. open-source web servers) that would, in-turn, serve other collaborative communities of millions of people building never-seen-before resources such as Wikipedia. The 10 forces described by Friedman have shaped the start of the 21st Century and continue to shape the world.

Friedman is not alone in his predictions of rapid change. Christensen, Horn and Johnson (2008) persuasively argue in *Disrupting Class: How Disruptive Innovation Will Change the Way the World Learns* that student-centric learning is expected as part of the trajectory of change realized through information technology. As schools explore opportunities to better meet student needs in economically challenging times, Christensen, Horn and Johnson suggest opportunities and pressures are present that will move education toward increased personalized attention thus better meeting specific learning needs and improving course and learning selection. The authors argue that personalized learning will occur in concert with effective use of information technologies as part of a broadly changed learning paradigm.

Other educational researchers also share in the vision of better meeting student needs through personalized learning. Leadbeater's (2005) work explores 'next practices' that are already occurring in school systems within the United Kingdom and suggests significant potential for personalized learning through schools collaborating to achieve this end, as well

as increased parental and student engagement in the interest of their perceived learning needs. Leadbeater's objective is to turn 'passive recipient' learners into active participants. Using an engagement process that encompasses learners, families, communities and schools, the end goal is to create learning environments that better meet learners' needs through a vested interest. This work, as others, suggests shifts in the paradigms of education and the use of information technology to achieve the end-goals.

While one may view such paradigm shifts as simply theoretical or not of pragmatic value, today's lead practicing educators demonstrate the value of integrating contemporary technologies to better meet student learning needs, often achieving a more personalized learning process. The use of contemporary technologies in these contexts frequently address such competencies as identified by leading thinkers such as Harvard Graduate School's Tony Wagner (2008) and organizations such as the partnership for 21st Century Learning. Each has closely examined the types of competencies needed by today's students. These competencies include learner development in such areas as communication and collaboration across networks, critical thinking and problem solving and creativity and innovation. Such competencies generally assume the use of technologies that engage students through the use of contemporary pedagogical approaches using contemporary learning tools (e.g. information technology).

Examples of practicing lead teachers who demonstrate the value of integrating contemporary technologies include winners of the Alberta Excellence in Teaching Award and Mr. Clarence Fisher, winner of the Prime Minister's Award for Teaching Excellence (2003).

Mr. Fisher's work, at EvenFromHere.org, exemplifies creating a classroom community – a community that explores the world using information technology as a connective tool to gather information about the world, understand the world, publish to the world and communicate and collaborate with others locally and in locations distant from Snow Lake, Manitoba. As shared by one of his students Mr. Fisher works to personalize learning (Government of Canada website, 2011):

> *He makes learning interesting by letting the students discuss viewpoints, instead of just teaching from the book. He tried to get to know his students so he could find out the kind of things they would like to do.*

His students are perceived as learners who will use today's tools to ready themselves for learning in tomorrow's settings.

Policy Insights

What does all of this suggest as one explores policy and procedure considerations? First, it suggests that one can anticipate change. As such, policy needs to provide direction and parameters, but also recognize flexible layers. If policy is tied tightly to specifics, it will rapidly fall out-of-date.

Second, it suggests policies must recognize the broader context in which they reside. Policies must meet the needs of stakeholders across the organization from students to educators to leaders.

Third, it suggests classrooms that offer tremendous learning potential – a world where information technology is a fundamental part of society and work, a tool for collaboration and communication, a means to creativity and innovation and a vehicle for problem solving and critical thinking.

Utilization Trends

Various authors speak of change and increased use of information technology within society. Hard data supports this view of dramatic shifts within society as access to information and pervasive connectedness to others has become normative around the world. While access to information per se has had a long history across the Internet, spanning several decades, pervasive connectedness with group communications and collaboration is a relatively new phenomenon. In today's working and social world, people's expectations regarding connectedness have changed. At this time, people expect others to have immediate access to the Internet and be capable of responding with similar immediacy. The broad trend of Internet connectivity from the Center for the Digital Future (Figure 3) shows the progressive increase of Internet access from 2000 to 2005. Shortly after 2005, a further impetus created additional demand for Internet services as Web 2.0 and social media technologies came to the forefront. Access again sprung ahead, spurred forward by the possibilities of these new collaborative and communication tools. In the Center's study of nearly 2,000 participants, when looking specifically at the population aged 12 years to 24 years of age, 100% of this age-range uses the Internet (Center for the Digital Future, 2010).

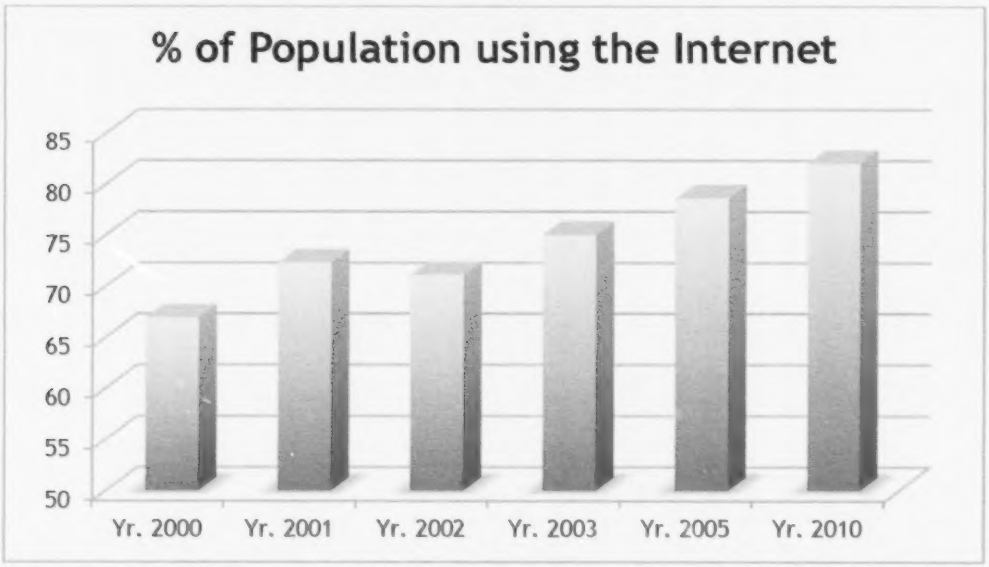


Figure 3. Trends in Internet Use (Center for the Digital Future at the Annenburg USC School, 2005 & 2010)

This incrementing trend is further shown in a Canadian context by Statistics Canada as its data illustrates Internet use by people 16 years and older in the years 2007 and 2009 (Figure 4). Even across these short time-frames the level of use increases across the nation and within each province. Alberta and British Columbia are the leading provinces in utilization of the Internet.

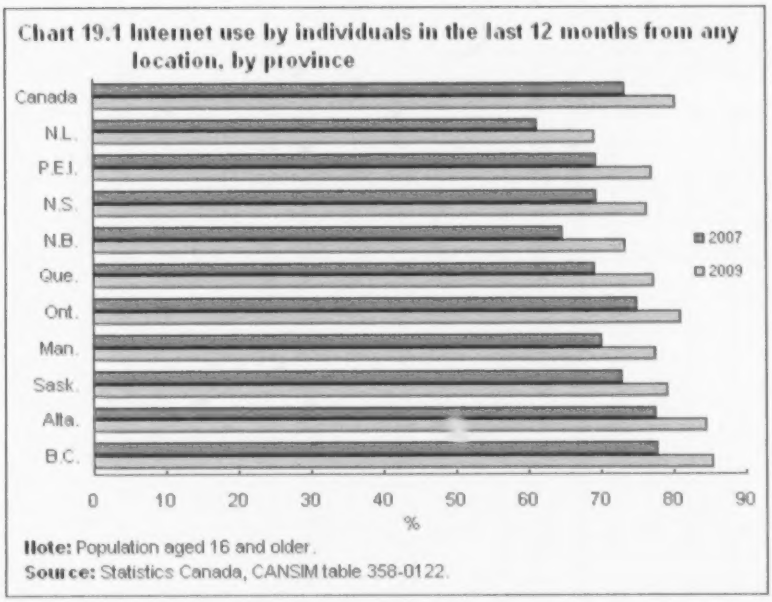


Figure 4. Canadian Internet Use in 2007 and 2009 by Province

The use of the Internet is by no means confined to students 16 years and older. Research by Livingstone & Haddon (2011) indicates that on average 9 to 16 year olds spend 88 minutes per day online. Lenhart et al's (2011) research indicates that 95% of teens aged 12 to 17 are Internet users, and that Internet usage among teens is higher than usage by adults as a whole.

Additionally, the type of online use has become increasingly individualized and privatized, often through mobile access. The type of access by children has changed. Nearly 50% of this group access the Internet in their bedroom and 33% use some form of personal device to access the Internet. Further, the report indicates that children are going online at younger and younger ages and that age restrictions on social networking sites are often ignored. This raises safety concerns, given that younger children may not be aware of the risks.

Canadian students largely have ready access to the Internet beyond the school. In a 2005 study of 5,272 students from across Canada, 94% indicate they have Internet access at home (Media Awareness Network, 2005). One can only assume this percentage has since increased. Beyond access, Canadian students also spend significant time online. In 2005, Grade 4 students were online a median of 2.4 hours per day; Grade 11 students were online 4.2 hours per day.

At a deeper level, the very nature of Internet use has changed dramatically over the course of the last few years. Ten years ago, Internet utilization tended to encompass gathering information from websites, e-mail and downloading files. A few technically capable educators and students posted information onto the web but beyond e-mail, the majority of users' focus was largely on searching and downloading information.

The dramatic shift in today's Internet use is the ability to instantly create, collaborate, communicate and problem-solve with others across the Internet. Such competencies have an obvious role within the education system. Further, it is recognized that student engagement and students' sense of community are critical variables related to student high school completion. The use of Web 2.0 tools (e.g. blogs, wikis, Voicethread, Vimeo) present educational opportunities for students that are both engaging and have potential for community building.

Pressures are coming forth on education systems as student personal use of social tools (e.g. Facebook, MySpace) has grown at a tremendous rate. Although students may or may not have such access at school, pending school authority policy, almost invariably they have such access outside of school. For example, Facebook, as one of the more popular social tools, is accessed by over 800 million active users. At least half of these active users use Facebook each day. More than 70 languages are used on the site. While nearly 17 million Canadians use Facebook, 73% of all users live outside of North America. A survey of 1,127 students (Masters in Education, 2011) indicates that 96% use Facebook – and, incidentally, 84% use YouTube.

While students utilize such tools as Facebook for social purposes, they are not nearly as likely to use Web 2.0 tools for educational purposes (e.g. blogs, wikis, Voicethread, Vimeo, Edmoto). Indeed, they are not as likely to be formally educated using Web 2.0 resources as they are to have freelance personal use of online social tools.

Policy Insights

Canadian society, and in particular Albertans, are accessing the Internet at very strong levels and at an increasing rate. Canadian and European data, as well as general observation, suggest children at younger and younger ages are accessing the Internet with frequency. Children are using online collaborative tools - independently of whether schools are adequately preparing them for such use. Given such high levels of utilization, questions need to be asked as to children's safety and preparedness if they fail to receive guidance or instruction in digital citizenship (Ohler, 2010).

Provincial Context

A number of provincial initiatives have demonstrated action in response to the broad set of changes occurring across society and in response to educational opportunity. While not all-inclusive, the following initiatives capture some of the current context within the province of Alberta.

Alberta SuperNet

Alberta students and educators are in a relatively unique situation. Through the Alberta SuperNet, over 400 communities are connected via a high-speed fibre-optic and wireless network. In total, 4,200 high-speed service locations are offered across the province. Over 2,000 of these offerings exist within the education sector. This level of connectivity encompasses all schools, municipalities and health services across the province. While bandwidth across the fibre is not open-ended, the underlying infrastructure brings tremendous access potential to students and educators.

Emerge One-to-One Laptop Learning Initiative

Use of the Alberta SuperNet within the education sector has been extensive and has enabled a breadth of learning and research projects. Building upon this high-speed network, the Emerge One-to-One Laptop Learning Initiative investigated the efficacy of employing laptops for teaching and learning. The laptops used for this project were connected to the Internet and many of them were connected wirelessly within each of the 20 different participating school divisions.

Numerous findings sprung from the extensive research associated with this project, both of a pedagogical and of a technical nature. While the findings are far too extensive to fully report in this guide, an example germane to the current topic is in order. With a very high level of frequency teachers reported that technology plays either a moderate role or a significant role in building skills or developing proficiencies in their students across subject areas. Given these technologies were largely highly connected and mobile, one may anticipate increased expectations from educators and students in accessing mobile connected technologies as part of the instructional tool set. These findings are detailed in Figure 5 below.

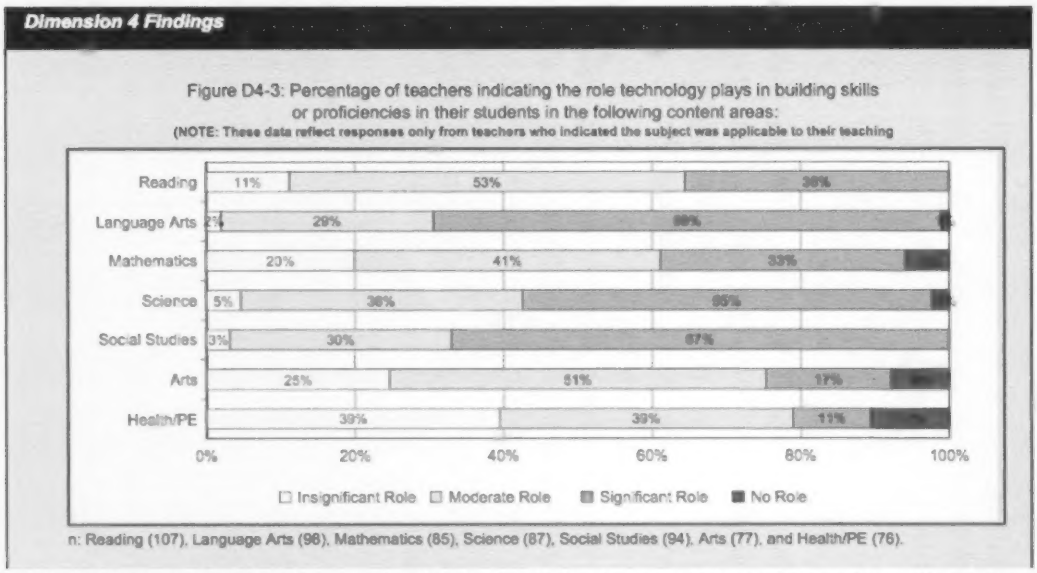


Figure 5. Percentage of teachers indicating technology plays a role in proficiency development across subject areas.

A complete description of findings from this research is found with the *Emerge One-to-One Laptop Learning Initiative: Final Report (2010)*.

College of Alberta School Superintendents' (CASS) 12th Dimension of the Framework for School System Success

In the Framework for School System Success, CASS underlines the significant role that leadership plays in developing excellent schools and ultimately excellent teaching. Through a series of associated activities, the framework is intended to build leadership capacity in Alberta.

As part of this broader CASS initiative, it has included a 12th dimension, which is a three-year initiative intended to build member capacity in 21st Century learning leadership – leadership which incorporates and guides information technology in educational settings.

This dimension, as one of 12 core elements in the CASS framework, addresses the need for supporting leaders in the development of 21st Century knowledge. The dimension recognizes the important role of 21st Century competencies, of developing IT governance and employing transformational leadership as a model for bringing change to school systems.

Bullying and Digital Citizenship

For several reasons, the topic of bullying deserves particular attention in the context of digital citizenship policy. First, Alberta's *School Act* (Alberta Queen's Printer, 2000) indicates clear responsibility to protect students. Addressing bullying within a digital context is highly recommended, given its perseverative nature, its global reach and the accessibility of victims, the anonymity of bullies, the disinhibition that sometimes occurs and the potentially serious, harmful effects on students (Olweus, N.D.). As well, cyberbullying and offline bullying are frequently related. One is often an extension of the other.

Second, bullying obviously does not occur only within a physical context or within a digital context. It may occur in either or both contexts. However, a significant challenge with the nature of bullying in a digital context is the perseverative nature of such bullying. Once a bullying comment, video, graphic or other harmful media element is released on the Internet, the material is nearly impossible to retract as it may be copied into other repositories across the Internet. Consequently, the victim may lack a vehicle for escaping a sense of being bullied ongoing, thus exacerbating psychological effects.

Third, research suggests that bullying is one of the most upsetting online risks that students face (Livingstone & Haddon, 2011). In a survey of over 25,000 students, researchers found that of all of the risks students might encounter when using the Internet, online bullying tended to upset children the most. Although online bullying is relatively rare (presently 6% online versus 19% offline), it is more upsetting for children than some of the issues that receive publicity and attention such as sexual images, sexual messages and meeting new people online.

Before exploring solutions to bullying, a definition of the term is in order. Olweus (N.D.) provides a helpful definition. He states,

> *A person is bullied when he or she is exposed, repeatedly and over time, to negative actions on the part of one or more other persons, and he or she has difficulty defending himself or herself.*
>
> *This definition includes three important components:*
> 1. *Bullying is aggressive behaviour that involves unwanted, negative actions.*
> 2. *Bullying involves a pattern of behaviour repeated over time.*
> 3. *Bullying involves an imbalance of power or strength.*

The risks of cyberbullying are seen to be on the rise. As noted within EU Kids Online,

> *Since risk increases as use (of the Internet) increases, it might seem simple to call for restrictions on children's use of the Internet. But online opportunities and digital literacy also increase with use, so there is no simple solution. Rather, ways must be found to manage risk without unduly restricting opportunities.* (p. 31)

The shocking outcomes from cyberbullying have been highlighted in the media with several instances resulting in youth suicide. Strategies are needed.

Part of the solution to meet the concern of cyberbullying, and bullying generally, among students resides in effective digital citizenship policies and instruction. Discussions within Alberta's Legislative Assembly suggest school boards have a responsibility in guiding student behaviours. Strategies to address bullying may include:

- Establishing meaningful digital citizenship policies to guide organizational members;
- Providing digital citizenship curricula to guide student learning;
- Providing professional development supports to guide teachers in this domain; and
- Ultimately, through the above process, providing supports for students as they encounter online learning experiences that expect digital citizenship.

By maintaining a learning focus, students and personnel will benefit from guidance into this new citizenship domain. Addressing the serious issue of bullying within schools is one of the benefits of digital citizenship policy development.

Policy Insights

Given extensive provincial leadership conversations identifying bullying problems and given extensive media attention to bullying, it seems prudent for school authorities to address bullying and cyberbullying within policy – particularly given the specific nature and perseverative effects of cyberbullying.

There is increasing recognition of the fluidity that now occurs between on-campus and off-campus student activities, often through digital connections. Responsibilities on behalf of students and on behalf of boards have tended to change to recognize this fluid interaction. Policies within school authorities will need to recognize such change in responsibility.

Appendix B: ISTE NETS for Digital Citizenship

NETS for Students

Permission granted: National Educational Technology Standards for Students, Second Edition, ©2007, ISTE® (International Society for Technology in Education), www.iste.org. All rights reserved.

Section 5. Digital Citizenship

Students understand human, cultural and societal issues related to technology and practice legal and ethical behaviour. Students:

a. advocate and practice safe, legal and responsible use of information and technology;
b. exhibit a positive attitude toward using technology that supports collaboration, learning;
c. demonstrate personal responsibility for lifelong learning;
d. exhibit leadership for digital citizenship.

For the complete NETS for Students please see:
http://www.iste.org/Content/NavigationMenu/NETS/ForStudents/2007Standards/NETS_for_Students_2007.htm

NETS for Teachers

Permission granted: National Educational Technology Standards for Teachers, Second Edition ©2008, ISTE® (International Society for Technology in Education), www.iste.org. All rights reserved.

Section 4. Promote and Model Digital Citizenship and Responsibility

Teachers understand local and global societal issues and responsibilities in an evolving digital culture and exhibit legal and ethical behaviour in their professional practices. Teachers:

a. advocate, model and teach safe, legal and ethical use of digital information and technology, including respect for copyright, intellectual property and the appropriate documentation of sources
b. address the diverse needs of all learners by using learner-centered strategies and providing equitable access to appropriate digital tools and resources
c. promote and model digital etiquette and responsible social interactions related to the

use of technology and information

d. develop and model cultural understanding and global awareness by engaging with colleagues and students of other cultures using digital-age communication and collaboration tools

For the complete NETS for Teachers please see:
http://www.iste.org/Content/NavigationMenu/NETS/ForTeachers/2008Standards/NETS_for_Teachers_2008.htm
http://www.iste.org/Libraries/PDFs/NETS_for_Teachers_2008_EN.sflb.ashx

NETS for Administrators

Permission granted: National Educational Technology Standards for Administrators, ©2009, ISTE® (International Society for Technology in Education), www.iste.org. All rights reserved.

Section 5. Digital Citizenship

Educational Administrators model and facilitate understanding of social, ethical and legal issues and responsibilities related to an evolving digital culture. Educational Administrators:

a. ensure equitable access to appropriate digital tools and resources to meet the needs of all learners;
b. promote, model and establish policies for safe, legal and ethical use of digital information and technology;
c. promote and model responsible social interactions related to the use of technology and information;
d. model and facilitate the development of a shared cultural understanding and involvement in global issues through the use of contemporary communication and collaboration tools.

For the complete NETS for Administrators please see:
http://www.iste.org/Content/NavigationMenu/NETS/ForAdministrators/2009Standards/NETS_for_Administrators_2009.htm

Appendix C: Personal Information: A FOIP Definition

The term *personal information* is a critical element within the *FOIP Act*. The definition according to the Act follows:

> *"Personal information" means recorded information about an identifiable individual, including*
>
> *a. the individual's name, home or business address or home or business telephone number,*
>
> *b. the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,*
>
> *c. the individual's age, sex, marital status or family status,*
>
> *d. an identifying number, symbol or other particular assigned to the individual,*
>
> *e. the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,*
>
> *f. information about the individual's health and health care history, including information about a physical or mental disability,*
>
> *g. information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,*
>
> *h. anyone else's opinions about the individual, and*
>
> *i. the individual's personal views or opinions, except if they are about someone else;*
>
> (Alberta Queen's Printer, 2009).

Appendix D: Digital Citizenship Needs Assessment Tool

The Digital Citizenship Needs Assessment Tool is provided in digital format to assist school authorities in examining their preparedness across all 11 digital citizenship elements, as identified within this guide, as well as items specific to a provincial context. The scale will demonstrate whether the school authority is well-positioned and which policy areas they may need to be address.

The Assessment takes approximately 20 to 30 minutes to complete.

Link to the Digital Citizenship Needs Assessment Tool:
http://www.education.alberta.ca/media/6731450/digital%20citizenship%20needs%20assessment%20tool.xlsx

References

Alberta Education. (2012a). Bring Your Own Device: A Guide for Schools. Retrieved June 25, 2012 from http://education.alberta.ca/media/6724519/byod guide final.pdf

Alberta Education. (2012b). Framework for Student Learning: Competencies for Engaged Thinkers and Ethical Citizens with an Entrepreneurial Spirit. Retrieved March 29, 2012 from http://education.alberta.ca/media/6581166/framework.pdf

Alberta Education. (2011a). *School Technology Services: Self-Evaluation Guide*. Retrieved January 10, 2012 from http://education.alberta.ca/media/6555222/school%20technology%20services%20-%20self%20evaluation%20guide-final.pdf

Alberta Education. (2011b). *Wireless Local Area Network (WLAN) Best Practices Guide*. Retrieved January 10, 2012 from http://education.alberta.ca/media/6607528/wireless guide 2011 publication edition.pdf

Alberta Education. (2010). *Emerge One to One Laptop Learning Initiative: Final Report*. Retrieved December 20, 2011 from http://education.alberta.ca/media/6343889/emerge final report 2010-10-17.pdf

Alberta Education Stakeholder Technology Branch. (2007). *Wireless Local Area Network Best Practices Guide*. Retrieved January 31, 2012 from http://education.alberta.ca/media/822010/wirelessbestpracticesguid.pdf

Alberta Education. (1999a). *Computer Network Security: Best Practices for Alberta School Jurisdictions*. Retrieved January 10, 2012 from http://www.albertaitmanagementservices.ca/docs/computernetworksecurity.pdf Security Policy, p. 7.

Alberta Education. (1999b). *Network Design: Best Practices for Alberta School Jurisdictions*. Retrieved January 10, 2012 from http://education.alberta.ca/media/618621/networkdesign.pdf

Alberta Queen's Printer. (2011). *The Legislative Assembly of Alberta Bill 18: Education Act*. Fourth Session, 27th Legislature, 60 Elizabeth II. 208 pp.

Alberta Queen's Printer. (2000). *Province of Alberta School Act*. Queen's Printer Bookstore, Edmonton, Alberta. 171 pp.

Alberta Queen's Printer. (2009 Revision). *Freedom of Information and Protection of Privacy Act: Revised Statutes of Alberta 2000, Chapter F-25.* Retrieved December 19, 2011 from http://www.qp.alberta.ca/documents/Acts/F25.pdf

boyd, d. (2008). *Taken Out of Context American Teen Sociality in Networked Publics.* Doctoral Dissertation, University of California - Berkley. Retrieved December 20, 2011 from http://www.danah.org/papers/TakenOutOfContext.pdf

boyd, d. (2009). *Answers to Questions on Teen Practices.* Retrieved December 22, 2011 from http://www.zephoria.org/thoughts/archives/2009/05/16/answers_to_ques.html

boyd, d. (2010). *Living Life in Public: Why American Teens Choose Publicity over Privacy.* AOIR 2010. Gothenburg, Sweden, October 23. Retrieved December 21, 2011 from http://www.danah.org/papers/talks/2010/AOIR2010.html

Branigan-Pipe, Z. (2011). *Parent Engagement and Social Media.* Retrieved December 15, 2011 from http://pipedreams-education.ca/2011/12/02/parent-engagement-and-social-media/

Calgary Board of Education. (2011). *Why Digital Citizenship?* – What is Digital Citizenship? Retrieved January 30, 2012 from http://www.innovativelearning.ca/sec-learntech/webaware-index.asp

Canada (2010). An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act. (40th parl., 3rd sess.) 20 Dec 2011. http://lois-laws.justice.gc.ca/eng/AnnualStatutes/2010_23/FullText.html

Canada (2011). An Act to amend the Copyright Act. Bill C-11, First Reading, Sep. 29, 2011 (41st parl., 2nd sess.) 23 Dec. 2011. http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5144516&File=9

Canadian Employment and Pension Law. (2011). *R v. Cole Update: Supreme Court of Canada grants leave to appeal.* Retrieved December 24, 2011 from http://www.canadianemploymentpensionlaw.com/employment/r-v-cole-update-supreme-court-of-canada-grants-leave-to-appeal/

Canadian Privacy Commissioner. (2011). *Securing Personal Information: A Self Assessment Tool for Organizations*. Retrieved January 25, 2012 from http://www.priv.gc.ca./resource/tool-outil/security-securite/english/AssessRisks.asp?x=1

College of Alberta School Superintendents. (2010). CASS Framework for School Systems Success.

Collins, J. (2001). *Good to Great: Why Some Companies Make the Leap...and Others Don't*. New York, NY: Harper Collins Publishing.

Christensen, Horn and Johnson (2008). *Disrupting Class: How Disruptive Innovation Will Change the Way the World Learns*. New York, NY: McGraw Hill

Churches, A. (2011). The Digital Citizen. Retrieved December 10, 2011 from http://edorigami.wikispaces.com/The+Digital+Citizen

Classroom 2.0 (2012). *Social Networking and Digital Citizenship*. Retrieved February 6, 2012 from http://www.classroom20.com/profiles/blogs/social-networking-and-digital-citizenship-3?xg_source=activity

Dooley, J. (2010). *Online Risks Clustered into Four Categories*. In Mira Danon-Baird (2010), Slide 11. Retrieved from http://www.slideshare.net/edgeoftheweb/embedding-digital-citizenship-into-curriculum

Donlevy, J., Chomos, J., Walker, K. (2008). *A Guide to Alberta School Law 2008*. Calgary, AB. 176 pp.

Fisher, C. (2011). *Even From Here Blog*. Retrieved November 9, 2011 from http://www.evenfromhere.org/

Fisher, C. (2010). *Do New Tools = New Learning?* Retrieved December 19, 2011 from http://www.evenfromhere.org/?p=1501

Friedman, T. (2005). *The World is Flat: A Brief History of the Twenty-First Century*. New York, NY: Farrar, Straus and Giroux.

Fullan, M. (2003). *The Moral Imperative of School Leadership*. Thousand Oaks, CA: Corwin Press Inc.

Fullan, M. (2001). *Leading in a Culture of Change*. San Francisco, CA: Jossey-Bass.

Garibaldi Secondary School. (2011). *Digital Citizenship Policy*. Retrieved January 10, 2012 from http://gss.sd42.ca/conduct/digital-citizenship-policy/

Global Kids, Harvard University's GoodPlay Project & Commons Sense Media (2009). *Meeting of Minds: Cross-Generational Dialogue on the Ethics of Digital Life*. Retrieved December 12, 2011 from http://www.macfound.org/atf/cf/%7Bb0386ce3-8b29-4162-8098-e466fb856794%7D/DML-FOCUS-DIALOGUE-REPORT-0910.PDF

Green, H. & Hannon, C. (2007). *Their Space: Education for a Digital Generation*. Demos, London. Retrieved October 11, 2011 from http://www.demos.co.uk/publications/theirspace

Harris Interactive. (2003). *Generation Y Earns $211 Billion and Spends $172 Billion Annually*. Retrieved November 2, 2011 from http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=667

Horton, M. & Thomson, J. (2008). Chapter 5: Canada. In the *Family Online Safety Institute, State of Online Safety Report* (pp. 61-72), FOSI, Washington, DC.

James, C., Davis, K., Flores, A., Francis, J., Pettingill, L., Rundle, M., Gardner, H. (2009). *Young People, ethics and the New Digital media: A Synthesis from the GoodPlay Project*. The John D and Catherine T. MacAurthur Foundation Reports on Digital Media and Learning. Retrieved December 13, 2011 from http://mitpress.mit.edu/books/full_pdfs/Young_People_Ethics_and_New_Digital_Media.pdf

Kay, K. & Greenhill, V. (2013). The Leader's Guide to 2st Century Education: 7 Steps for Schools and Districts. Pearson Education Inc., New Jersey.

Leadbeater, C. (2005). *The Shape of Things to Come: Personalised Learning through Collaboration*. The Department for Education and Skills (DfES), Nottingham, UK.

Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, & K., Raine, L. (2011). *Teens, Kindness and Cruelty on Social Network Sites*. Washington, D.C.: Pew Research Center. Retrieved December 1, 2011 from http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx

Lencioni, P. (2002). *The Five Dysfunctions of a Team: A Leadership Fable*. San Francisco: Jossey-Bass.

Levinson, M. & Socia, D. (2010) *Moving Beyond One Size Fits All with Digital Citizenship.* Retrieved December 10, 2011 from http://publius.cc/moving_beyond_one_size_fits_all_digital_citizenship

Living Center Artist Collaboratives. (2012) Retrieved January 9, 2012 from http://www.newenglandvillage.org/gallery_collaboratives.html

Livingstone, S. & Haddon, L. (2011). *EU Kids Online: September 2011.* The London School of Economics and Political Science, London, United Kingdom. 52 pp.

Mashup Awards. (2009). Retrieved January 9, 2012 from http://mashupawards.com/winners/

Masters in Education (2011). *Infographic: How to Get Better Grades Using Social Media.* Retrieved February 1, 2011 from http://mastersineducation.org/infographic-how-to-get-better-grades-through-social-media/

NATO Review. (2011). Political change: what social media can – and can't do. Retrieved December 14, 2011 from http://www.nato.int/docu/review/2011/Social_Medias/Social_media_can_do/EN/index.htm

Ohler, J. (2011). Digital Citizenship Means Character Education for the Digital Age. *Kappa Delta Pi Record*, Fall 2011. Retrieved January 17, 2012 from http://www.kdp.org/publications/pdf/record/Centennial/Ohler.pdf

Ohler, J. (2010). *Digital Community: Digital Citizen.* Thousand Oaks, CA: Corwin Press.

Olweus (N.D.) *What is Cyberbullying?* Retrieved December 22, 2011 from http://www.olweus.org/public/cyber_bullying.page?menuheader=1

Ontario College of Teachers. (2011). *Professional Advisory: Use of Electronic Communication and Social Media.* Retrieved November 15, 2011 from http://www.oct.ca/publications/PDF/Prof_Adv_Soc_Media_EN.pdf

Ontario Court of Appeals. (2011). *R. v. Cole, 2011 ONCA 218.* Retrieved December 20, 2011 from http://www.ontariocourts.on.ca/decisions/search/en/OntarioCourtsSearch_VOpenFile.cfm?serverFilePath=D%3A%5CUsers%5COntario%20Courts%5Cwww%5Cdecisions%5C2011%5C2011ONCA0218%2Ehtm

Portsmouth School District. (2010). *Portsmouth School Board Policy Manual: Acceptable Use Policy*. Retrieved December 15, 2011 from http://www.cityofportsmouth.com/school/policies/PortsmouthSchoolBoardPolicyManual.pdf

Quillen, I. (2011). *Districts Tackle Questions Surrounding BYOT Policy: "Bring-your-own-technology" efforts in schools raise questions about what works*. Retrieved October 28, 2011 from http://www.edweek.org/dd/articles/2011/10/19/01byot.h05.html?tkn=XQMFK8w3LwSX4BsHUHOdQcTux2uXOjD6VQoq&cmp=ENL-EU-VIEWS1

RIAA v. The People: Five Years Later. (2008). Retrieved November 1, 2011 from https://www.eff.org/wp/riaa-v-people-five-years-later

Ribble, M. (2011). *Digital Citizenship in Schools (2nd ed.)*. Eugene, OR: International Society for Technology in Education (ISTE).

Ribble, M. (2009). *Raising a Digital Child*. Retrieved December 12, 2011 from http://www.awaymagazine.be/family

Rockyview School Division. (2011). *Policy IFCL: Digital Citizenship*. Retrieved January 20, 2012 from http://www.rockyview.ab.ca/board_policies/ourboardandpolicies/board-policies/IFCL-DigitalCitizenship.pdf

Rose, D. & Meyer, A. (2002). *Teaching every student in the digital age: Universal Design for Learning*. Alexandria, VA: Association for Supervision and Curriculum Development.

Saenz, A. (2009). *Finland Guarantees Right to Broadband Internet Access*. Singularity Hub, October 15, 2009. Retrieved December 14, 2011 from http://singularityhub.com/2009/10/15/finland-guarantees-right-to-broadband-internet-access/

Solove, D. (2007). *The Future of Reputation: Gossip, Rumor and Privacy on the Internet*. New Haven, CT: Yale University Press. (Retrieved December 20, 2011 from http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text.htm)

Turiel, E. (2002). *The Culture of Morality: Social Development, Context and Conflict*. New York: Cambridge University Press.

USC Annenberg School for Communication & Journalism. (2011). *2010 Digital Future*

Report: Tenth Study by the Digital Future Project Finds High Levels of Concern about Corporate Intrusion in Personal Lives. Retrieved October 31, 2011 from http://www.digitalcenter.org./pdf/2011_digital_future_final_release.pdf

United States. Cong. Senate. 107th Congress, 1st Session. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001." (as introduced in the U.S. Senate 23 October 2001). Retrieved December 19, 2011 from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf.

United Nations General Assembly. (2011). *Human Rights Council: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/17/27*. Retrieved December 14, 2011 from http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Wolf Creek Public Schools. (2009). *Administrative Procedure #169: Protection of Personal Information and Privacy*. Retrieved January 23, 2012 from http://www.wolfcreek.ab.ca/Procedures100?object=/documents_directory/Procedures%20(admin)/Section%20100%20General%20Administration&inforbar=no%templates=rwd&confposition=2

Wright, S. (2011). *Wright's Room*. Retrieved December 23, 2011 from http://shelleywright.wordpress.com/

Young, K. (2009). The *Center for Internet Addiction*. Retrieved January 11, 2012 from http://www.netaddiction.com/

ZDNet. (2007). *The Internet's New Dr. Spock*. Retrieved December 12, 2011 from http://www.zdnet.com/news/the-internets-new-dr-spock/160171

Zuckerman, E. (2011). *The 2011 Vancouver Human Rights Lecture*. Retrieved December 14, 2011 from http://www.youtube.com/watch?v=tkDFVz_VL_I